

On cubic action of a rank one group

Matthias Grüninger*
 Universität Bielefeld
 Fakultät für Mathematik
 Universitätsstraße 25
 33615 Bielefeld
 E-Mail: mgruenin@math.uni-bielefeld.de

July 15, 2011

Abstract

We consider a rank one group $G = \langle A, B \rangle$ which acts cubically on a module V , this means $[V, A, A, A] = 0$ but $[V, G, G, G] \neq 0$. We assume that $A_0 := C_A([V, A]) \cap C_A(V/C_V(A))$ is not trivial; this is always the case if A is not abelian. Then A_0 defines a subgroup G_0 of G which acts quadratically on V . By a theorem of Timmesfeld $G_0 \cong SL_2(J, R)$ for a ring R and a special quadratic Jordan division algebra $J \subseteq R$. We show that J is either a Jordan algebra contained in a commutative field or a hermitian Jordan algebra. In the second case G is the special unitary group of a pseudo-quadratic form π of Witt index 1.

Keywords: Rank one groups, Moufang sets, pseudo-quadratic forms

1 Introduction

Abstract rank one groups were introduced by Franz Georg Timmesfeld in [15].

Definition 1.1 *A group G with two distinct nilpotent subgroups A and B is called an abstract rank one group with unipotent subgroups A and B if $G = \langle A, B \rangle$ and if for all $a \in A^\#$ there is an element $b(a) \in B^\#$ with $B^a = A^{b(a)}$ and vice versa.*

The most common example for a rank one group is the group $SL_2(K)$ with K a (skew-)field and A and B the group of lower resp. upper unipotent matrices 2×2 - matrices over K . Alternatively, one can take $G = PSL_2(K)$.

The concept of an abstract rank one group is closely related to the concept of a Moufang set. A Moufang set is a pair $(X, (U_x)_{x \in X})$, where X is a set with at least 3 elements and $(U_x)_{x \in X}$ is a family of subgroups of $Sym X$ such that U_x

*Supported by DFG-Grant GZ BA 2200//3-1 "Moufang sets and split BN-pairs of rank one"

fixes x and acts regularly on $X \setminus \{x\}$ and such that $U_x^g = U_{xg}$ for all $x, y \in X$ and all $g \in U_y$. The groups U_x are called *root groups* and the group $G^\dagger = \langle U_x; x \in X \rangle$ is called the *little projective group* of the Moufang set. If $(X, (U_x)_{x \in X})$ is a Moufang set with nilpotent root groups, then G^\dagger is an abstract rank one group with unipotent subgroups U_x and U_y for all $x, y \in X$ with $x \neq y$. Conversely, if $G = \langle A, B \rangle$ is a rank one group, then $(X, (U_x)_{x \in X})$ with $X = \{A^g; g \in G\}$ and $U_{A^g} = A^g Z(G)/Z(G)$ is a Moufang set with $G^\dagger = G/Z(G)$. So a rank one group is a central extension of the little projective group of a Moufang set with nilpotent root subgroups. Note that not every central extension of G^\dagger is a rank one group. If for example $G = A_5$ and $A, B \in \text{Syl}_2(G)$, then G is a rank one group with unipotent subgroups A and B and $Z(G) = 1$, but $\tilde{G} = \langle \tilde{A}, \tilde{B} \rangle$ with $\tilde{G} = \text{SL}_2(5)$ and with preimages \tilde{A}, \tilde{B} of A and B in \tilde{G} is not a rank one group with unipotent subgroups \tilde{A} and \tilde{B} . We refer to [17] where the notion of a rank one extension is introduced.

There is a strong connection between rank one groups and *quadratic pairs* (see [15]). A quadratic pair consist of a finite-dimensional k -vectorspace V (k a field of odd characteristic) and a subgroup G of $\text{GL}_k(V)$ generated by quadratic elements, i.e. elements with minimal polynomial $(X - 1)^2$. We further assume that if $\varphi \in \text{End}_k(V)$ with $\varphi^2 = 0$ and $\text{id}_V + \varphi \in G$, then also $\text{id}_V + \lambda\varphi \in G$ for all $\lambda \in k$. Note that if $\text{char } k = 2$, then an element in $\text{GL}(k, V)$ is quadratic iff it is an involution. Generalizing this concept, we define

Definition 1.2 ([17]) *Let $G = \langle A, B \rangle$ be a rank one group. A $\mathbb{Z}G$ -module V is called quadratic if $[V, A, A] = 0$ but $[V, G, G] \neq 0$.*

Rank one groups possessing a quadratic module are sometimes called quadratic. Since $G = NA$ or $N \cap A = 1$ for every normal subgroup N of G (by I(1.10) of [16]), the condition $[V, G, G] \neq 0$ implies that A acts faithfully on V . Note that if $[V, G] = V$, then V is either an elementary-abelian p -group or torsion free and uniquely divisible, so V is a k -vectorspace for $k = \mathbb{F}_p$ or $k = \mathbb{Q}$. Both $\text{char } k = 2$ and $\dim_k V = \infty$ are allowed.

The most common example for this situation is $G = \text{SL}_2(K)$ and $V = K^2$ for a (not necessarily commutative) field K . One can generalize this as follows: Let R be a ring with 1. A subgroup J of $(R, +)$ is called a special quadratic Jordan division algebra if $1 \in J$ and if $a \in J^\# = J \setminus \{0\}$, then a is invertible in R and a^{-1} is again in J . Note that the Hua identity implies that $bab \in J$ for all $a, b \in J$ [8]. Set

$$A := \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}; a \in J \right\}, B := \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}; a \in J \right\}$$

and $\text{SL}(J, R) = \langle A, B \rangle$. Then $\text{SL}(J, R)$ is a rank one group with unipotent subgroups A and B and $V = R^2$ is a quadratic module for $\text{SL}(J, R)$.

Timmesfeld showed that every quadratic rank one group is isomorphic to $\text{SL}_2(J, R)$ for a special quadratic Jordan division algebra inside a ring R .

Theorem 1.3 ([17], Theorem 1.1.) *Let $G = \langle A, B \rangle$ be a rank one group which acts quadratically on a module V . Set $W := [V, G]/(C_V(G) \cap [V, G])$,*

$X = [W, A]$ and $R = \text{End}(X)$. Then there is a special quadratic Jordan division algebra $J \subseteq R$ such that $G \cong SL_2(J, R)$.

Quadratic Jordan division algebras were classified by McCrimmon and Zel'manov (15.7 in [11]): Every special quadratic Jordan division algebra is isomorphic to the quadratic Jordan algebra of a skewfield, an ample hermitian Jordan algebra or a Jordan algebra of Clifford type (note that these families are not disjoint). We therefore get a classification of all quadratic rank one groups.

This result can be seen as a special case of the more general conjecture that every special Moufang set with abelian root groups (equivalently (by [12]), every Moufang with abelian root groups and G^\dagger not sharply 2-transitive) is isomorphic to the Moufang set of quadratic Jordan division algebra (see [4]).

In [15] Timmesfeld classified all quadratic pairs (V, G) such that G contains two distinct commuting root groups. This leaves the case that G contains no commuting root subgroups. Concretely, this means that V is a finite-dimensional vectorspace over a field k of odd characteristic and G is a subgroup of $GL_k(V)$ generated by a set Σ of subgroups of G such that for all $A, B \in \Sigma, A \neq B$ the group $\langle A, B \rangle$ is a rank one group with unipotent subgroups A and B which acts quadratically on V . Such groups were examined in [18]. The author showed that if 3 is the minimal number of elements of Σ which are needed to generate G , then one of the following cases hold:

- (a) There is a quadratic extension K/k with Galois group $\langle \sigma \rangle$ and a σ -hermitian form $f : K^3 \times K^3 \rightarrow K$ with Witt index 1 such that $G \cong SU_3(K, f)$.
- (b) There is a division algebra K over k with involution σ and a σ -hermitian form $f : K^3 \times K^3 \rightarrow K$ such that $G \cong SU_3(K, f)$. Moreover, $K_\sigma = \{x \in K; x^\sigma = x\}$ generates K as a ring.

If $A, B \in \Sigma$ are different, then the special quadratic Jordan division algebra associated to $\langle A, B \rangle$ is k^+ in the first case and K_σ in the second case.

To prove this result, Timmesfeld introduced the group $U(A)$ for $A \in \Sigma$.

$$U(A) := \{g \in G; [V, g] \subseteq C_V(A), [C_V(A), g] \subseteq [V, A] \text{ and } [V, A, g] = 0\}.$$

He showed that if $A, B \in \Sigma, A \neq B$, then G is a rank one group with unipotent subgroups $U(A)$ and $U(B)$. The group $U(A)$ acts 'cubically' on V , this means $[V, U(A), U(A), U(A)] = 0$. This motivates the following definition:

Definition 1.4 *Let G be a rank one group with unipotent subgroups A and B . A $\mathbb{Z}G$ -module V is called a cubic module for G if $[V, A, A, A] = 0$, but $[V, G, G, G] \neq 0$.*

Here again, we will later see that one can assume that V is a kG -module for a field k . Both $\text{char } k = 2$ and $\dim_k V = \infty$ are allowed. Note that we don't exclude that $[V, A, A] = 0$ (and so V is actually a quadratic module for V). But if A is not abelian, then $[V, A, A] = 0$ implies $C_A(V) \neq 0$, so $C_G(V) \neq 0$ and

thus $G = C_G(V)A$ by I(1.10) of [16], hence $[V, G, G, G] = [V, A, A, A] = 0$. If $G = \langle A, B \rangle$ acts cubically on V and A is not abelian, then there is a root subgroups A_0 of A and B_0 of B with $A_0 \leq Z(A)$, $B_0 \leq Z(B)$ and $[V, B, B_0] = [V, B_0, B] = 0 = [V, A, A_0] = [V, A_0, A]$. Thus $G_0 = \langle A_0, B_0 \rangle$ is a rank one group which acts quadratically on V . In the notation of Timmesfeld, one has $U(A_0) = A$ and $U(B_0) = B$. By 1.3 $G_0 = SL_2(J, R)$ for a ring R and a special quadratic Jordan division algebra $J \subseteq R$. We will show that either J is a commutative Jordan algebra (and so either J is the Jordan algebra of a commutative field or there is a non-perfect field F with $\text{char} F = 2$ such that $F^2 \subseteq J \subseteq F$) or $J \cong H_0(K, *)$ for a skewfield K with involution $*$ such that $H_0(K, *)$ generates K . In the second case there is a K -vectorspace X and a pseudo-quadratic form $\pi : X \rightarrow K/H_0(K, *)$ of Witt index 1 such that $G \cong SU(\pi)$. Moreover, if $[V, G] = V$, $C_V(G) = 0$ and if $\text{char} K \neq 2$ or K is neither a quaternion algebra nor a biquaternion algebra, then V is the direct sum of G -modules isomorphic to X . This result is similar to the following: If Δ is the generalized quadrangle corresponding to an involutory set (K, K_0, σ) with $\sigma \neq 1$ and $\langle K_0 \rangle = K$ and if Γ is an extension of Δ (in the sense of (21.5) in [19]), then by (21.11) of the same book there is a K -vectorspace L_0 and an anisotropic pseudo-quadratic form $\pi : L_0 \rightarrow K/K_0$ such that Γ is the generalized quadrangle corresponding to π .

If J is commutative, the situation more complicated. The standard example for this case are unitary groups over commutative fields or quaternion division algebras, but there are other example as those resulting from quadratic forms of type E_6, E_7 and E_8 (see 3.6). Moreover, for E_6 and E_7 the corresponding Moufang sets are isomorphic to unitary Moufang sets (see [3]). Therefore it is possible that a rank one group acts cubically on two non-isomorphic irreducible modules

The paper is organized as follows: In Section 2 we repeat some facts about rank one groups and some facts about algebra we will need (semi-prime rings, skewfields with involution, pseudo-quadratic forms). Moreover, we will prove a ring-theoretical lemma we will use in Section 4. In Chapter 3 we will prove some elementary facts about cubic action. Especially we will introduce the subgroup A_0 of A and the 'normal form' of a cubic module. In Section 4 we will introduce the rings R and S which are contained in $\text{End}(C_V(A))$. We will show that R is (almost always) a skewfield and give a criterion when $R = S$ holds. In Section 5 we will show how to find irreducible modules inside a cubic module and give a criterion when a module is totally reducible. In Section 6 we will construct an anisotropic pseudo-quadratic form on A/A_0 (which is always a R -module). Using the methods in Section 7, we will transform this form to a pseudo-quadratic form of Witt index 1 on an irreducible subspace of our cubic module.

2 Preliminaries

2.1 Rank one groups and Moufang sets

We will assume that G is a rank one group with unipotent subgroups A and B . As mentioned in the introduction, this means that there are functions $A^\# \rightarrow B^\# : a \mapsto b(a)$ and $B^\# \rightarrow A^\# : b \mapsto a(b)$ with $A^{b(a)} = B^a$ and $B^{a(b)} = A^b$. One sees immediately that $a(b(a)) = a$ and $b(a(b)) = b$ for all $a \in A^\#$ and all $b \in B^\#$ holds.

Definition 2.1 For all $a \in A^\#$ set $\mu_a := b(a^{-1})ab(a)^{-1}$.

One easily computes $A^{\mu_a} = B$ and $B^{\mu_a} = A$. Moreover, μ_a is the unique element in the double coset BaB with this property.

Definition 2.2 Set $H = \langle \mu_a \mu_b; a, b \in A^\# \rangle$. Then H is called the Hua subgroup of G .

Since μ_a interchanges A and B , H is contained in $N_G(A) \cap N_G(B)$. One can show that $H = N_G(A) \cap N_G(B)$ (3.1 (ii) in [5]).

We recall that a rank one group $G = \langle A, B \rangle$ is called *special* if $b(a)^{-1} = b(a^{-1})$ for all $a \in A^\#$. A rank one group is special iff the corresponding Moufang set is special (see [4] for the definition of a special Moufang set).

Definition 2.3 A subgroup A_0 of A is called a root subgroup if the set $B_0 := \{1\} \cup \{b(a); a \in A_0^\#\}$ is a subgroup of B .

If A_0 is a root subgroup of A , then $G_0 := \langle A_0, B_0 \rangle$ is rank one group with unipotent subgroups A_0 and B_0 . We say that A_0 is a special root subgroup if the rank one group G_0 is special.

A Moufang set is called *non-proper* if the little projective group G^\dagger is sharply 2-transitive.

2.2 Some ring theory

A ring R is called *semi-prime* if R has no nilpotent ideals, this means that if I is an ideal of R with $I^n = 0$ for a natural number $n \geq 1$, then $I = 0$. We set $\mathfrak{B}(R) := \bigcap \{I; I \trianglelefteq R, R/I \text{ semi-prime}\}$. One easily sees that $R/\mathfrak{B}(R)$ is semi-prime, so $\mathfrak{B}(R)$ is the smallest ideal of R such that the factor ring is semi-prime. $\mathfrak{B}(R)$ is called the (lower) *Baer radical* of R (see [1]). It is contained in the Jacobson radical of R and every element of $\mathfrak{B}(R)$ is nilpotent, so an element $x \in R$ is a unit iff $x + \mathfrak{B}(R)$ is a unit in $R/\mathfrak{B}(R)$.

The following lemma is a generalization of 14.1.1 in [13], where both S and R are skewfields (and so $I_{x+1} = 0$).

Lemma 2.4 Let S be a ring with 1 and let R be a subring of S with $1 \in R$. Suppose there is a unit $x \in S$ such that $x + 1$ is again a unit and such that $x^{-1}Rx = (x + 1)^{-1}R(x + 1) = R$. Then $(x + 1)^{-1} \in R$ or $I_{x+1} := R \cap (x + 1)R$ is an ideal of R with $I_{x+1} \neq R$ and $x^{-1}ux - u \in I_{x+1}$ for all $u \in R$.

Proof. Let $u \in R$, set $v := x^{-1}ux$ and $w := (x+1)^{-1}u(x+1)$. Thus $xv = ux$ and $(x+1)w = u(x+1)$. We get $(x+1)v - v + u = xv + u = ux + u = u(x+1) = (x+1)w$ and hence $(x+1)(v-w) = v-u \in I_{x+1}$. Since $I_{x+1} = (x+1)R \cap R = (x+1)(x+1)^{-1}R(x+1) \cap R = R(x+1) \cap R$, I_{x+1} is an ideal of R . If $I_{x+1} = R$ then $1 \in (x+1)R$ and thus $(x+1)^{-1} \in R$. If $I_{x+1} \neq R$, then $x^{-1}ux - u \in I_{x+1}$ for all $u \in R$ and thus x centralizes R/I_{x+1} . \square

2.3 Special quadratic Jordan algebras

Let K be a field and R a K -algebra. For $a \in R$ we define the linear map $Q_a : R \rightarrow R : b \mapsto aba$ and set $Q_{a+b} = Q_a + Q_b$ for $a, b \in R$. Then a subspace $J \subseteq R$ is called a *special quadratic Jordan algebra* if $JQ_a \subseteq J$ for all $a \in J$. Of course R itself is a special quadratic Jordan algebra; we denote it by R^+ . If R is unital and $1 \in J$, then J is called *unital*. If J is unital, then J is called a *division algebra* if all element of $J^\# = J \setminus \{0\}$ are invertible in R and if $a^{-1} \in J$ for all $a \in J^\#$. The subgroup of $GL(J)$ generated by the maps Q_a for $a \in J^\#$ is called the *inner structure group* of J .

If J, J' are special quadratic Jordan algebras over a field K , then a map $f : J \rightarrow J'$ is called a *Jordan homomorphism* if it is K -linear and if $f(bQ_a) = f(b)Q_{f(a)}$ for all $a, b \in J$. If J is a special quadratic Jordan algebra over K , R is a K -algebra and $f : J \rightarrow R$ is an injective Jordan homomorphism such that $f(J)$ generates R as a ring, then (R, f) is called an *envelope* for J . An envelope (R, f) of J is called *universal* if for any other envelope (S, g) of J there is a K -algebra homomorphism $\varphi : R \rightarrow S$ with $\varphi \circ f = g$. One can construct a universal envelope as follows: Let $T(J) = K \oplus J \oplus (J \otimes_K J) \oplus (J \otimes_K J \otimes_K J) \dots$ be the tensor algebra over J and let $I(J)$ be the ideal generated by all elements of the form $bQ_a - a \otimes b \otimes a$ and by $1_K - 1_J$. Then $T(J)/I(J)$ together with the canonical embedding $a \mapsto a + I(J)$ is a universal envelope of J . This construction depends on the choice of K . If F is a subfield of K , then J is also a Jordan algebra over F , and it is not clear if the universal envelope over F equals the universal envelope over K . We show

Lemma 2.5 *Let J be a Jordan division algebra over a field K and let F be a subfield of K . Let (U_K, f) resp. (U_F, g) be universal envelopes of J over K resp. F . Then there is an epimorphism $\varphi : U_F \rightarrow U_K$ with $\varphi \circ g = f$ such that $\ker \varphi \subseteq \mathfrak{B}(U_F)$.*

Proof. Since U_K is also an envelope of J over F , the existence of a homomorphism $\varphi : U_F \rightarrow U_K$ with $\varphi \circ g = f$ follows by the property of the universal envelope. Since $f(J)$ generates U_K , φ must be onto. Since J is a division algebra, $g(J) \cap \ker \varphi = 0$. We have to show that $g(\lambda a) - g(\lambda 1_J)g(a) \in \mathfrak{B}(U_F)$ and that $g(\lambda 1_J) + \mathfrak{B}(U_F) \in Z(U_F/\mathfrak{B}(U_F))$ for all $a \in J$ and all $\lambda \in K$. If R is a ring containing J , then we set $[a, b] := ab - ba$ and $[a, b, c] := [[a, b], c]$ for $a, b, c \in R$. Then (0.25) and (0.27) of [11] imply $[a, b]^2, [a, b, c] \in J$ and $g([a, b]^2) = [g(a), g(b)]^2$, $g([a, b, c]) = [g(a), g(b), g(c)]$ for all $a, b, c \in J$. If $\text{char} K = 2$, then $[a, b] \in J$ and $g([a, b]) = [g(a), g(b)]$ for all $a, b \in J$.

If $\text{char}K \neq 2$, then for $a \in J$ and $\lambda \in K$ this implies $[g(\lambda 1_J), g(a)] \in Z(U_F)$ and $[g(\lambda 1_J), g(a)]^2 = 0$. Thus the image of $\lambda 1_J$ in $U_F/\mathfrak{B}(U_F)$ is in the center of this ring. Since g is a Jordan homomorphism, we have

$$g(\lambda a) = \frac{1}{2}(g(\lambda 1_J)g(a) - g(a)g(\lambda 1_J)).$$

Thus, we get

$$g(\lambda a) + \mathfrak{B}(U_F) = g(\lambda 1_J)g(a) + \mathfrak{B}(U_F) = g(a)g(\lambda 1_J) + \mathfrak{B}(U_F).$$

Thus the claim follows.

Assume that $\text{char}K = 2$. Then $g(\lambda 1_J) \in Z(U_F)$ and

$$[g(a^{-1}), g(\lambda a)] = g([\lambda a^{-1}, a]) = 0$$

for all $\lambda \in K$ and all $a \in J$. Let $a \in J^\#$, $\lambda \in K^*$ and set $u := g(\lambda a)g(\lambda^{-1}1_J)g(a^{-1})$. Then

$$\begin{aligned} ug(b)u &= g(\lambda a)g(\lambda^{-1}1_J)g(a^{-1})g(b)g(a^{-1})g(\lambda^{-1}1_J)g(\lambda a) \\ &= g(bQ_{a^{-1}}Q_{\lambda^{-1}1_J}Q_{\lambda a}) = g(b). \end{aligned}$$

Moreover,

$$[g(b), g(\lambda a)g(a^{-1})] = g(b)g(\lambda a)g(a^{-1}) + g(a^{-1})g(\lambda a)g(b) = g(\lambda aQ_{b,a^{-1}}) = 0,$$

hence $g(\lambda a)g(a^{-1}) \in Z(U_F)$ and so $u \in Z(U_F)$. So $u - 1$ is a nilpotent element in $Z(U_F)$ and thus contained in $\mathfrak{B}(U_F)$. Thus we have

$$g(\lambda a) + \mathfrak{B}(U_F) = g(\lambda 1_J)g(a) + \mathfrak{B}(U_F) = g(a)g(\lambda 1_J) + \mathfrak{B}(U_F).$$

□

If U is the universal envelope of J , then we call $U/\mathfrak{B}(U)$ the universal semiprime envelope of J . This definition doesn't depend on the ground field K by the previous lemma.

Proposition 2.6 *Let J be a special quadratic Jordan division algebra. Then the following statements are equivalent.*

- (a) $J \cong F^+$ for a commutative field F or there is a commutative field F of characteristic 2 and a F^2 - subspace J' with $F^2 \subseteq J' \subseteq F$ such that $J \cong J'$.
- (b) The universal semiprime envelope of J is a commutative field.
- (c) There is a commutative envelope R for J .
- (d) The inner structure group of J is abelian.

Proof. If $J = F^+$ for a commutative field F , then $\dim_F J = 1$ and so one easily sees that F is the universal F -envelope of J . Suppose $F^2 \subseteq J \subseteq F$ for a commutative field F with $\text{char} F = 2$ and let $U = T(J)/I(J)$ the universal F^2 -envelope of J . Then for all $a, b \in J$ we have $a^2 - a \otimes a \in I(J)$ and thus

$$(a+b)^2 - (a+b) \otimes (a+b) - (a^2 - a \otimes a) - (b^2 - b \otimes b) =$$

$$a^2 + b^2 + a \otimes a + b \otimes b + a \otimes b + b \otimes a + a^2 + a \otimes a + b^2 + b \otimes b = a \otimes b + b \otimes a \in I(J).$$

This shows that U is commutative. Since F is an envelope for J , there is a homomorphism $\varphi : U \rightarrow F$ with $\varphi(a) = a$ for all $a \in J$. The kernel of φ is generated by all elements $ab - a \otimes b + I(J)$ with $a, b, ab \in J$. Since $a \otimes b + b \otimes a \in I(J)$, we get

$$(ab - a \otimes b)^2 + I(J) = a^2 b^2 + a \otimes b \otimes a \otimes b + I(J) = a^2 b^2 + a \otimes a \otimes b \otimes b + I(J) = a^2 b^2 + a^2 b^2 = 0.$$

This shows that $\ker \varphi$ is a nilpotent ideal and so the semiprime envelope of J is just F . Thus we have shown that (a) implies (b).

The implications (b) to (c) and (c) to (d) are trivial. For the remaining implication (d) to (a) we can apply the classification of Jordan division algebras ([11], 15.7). Alternatively, every Jordan division algebra J defines a special Moufang set $M(J)$ and the Hua group of $M(J)$ is just the inner structure group of J ([5], 4.1 and 4.2). Thus (d) to (a) is a consequence of 6.1 in [5] and the main theorem of [6]. \square

2.4 Involutory sets and pseudo-quadratic forms

If K is a skewfield with involution $*$, then we set $H(K, *) := \{x \in K; x^* = x\}$. An additive subgroup $H_0(K, *)$ of $H(K, *)$ is called an ample Hermitian Jordan algebra if $1 \in H_0(K, *)$ and $x^* H_0(K, *) x \subseteq H_0(K, *)$ for all $x \in K$. $H_0(K, *)$ is a special quadratic Jordan division algebra since $x^{-1} = x^{-*} = x^{-*} x x^{-1} \in H_0(K, *)$ for all $x \in H_0(K, *)$. Note that $x + x^* = (x+1)^*(x+1) - x^* x - 1 \in H_0(K, *)$ for all $x \in K$. Set $K_* := \langle x^* x; x \in K \rangle$. Then K_* is the smallest Hermitian Jordan algebra relative to $*$. If $\text{char} K \neq 2$, then $x = \frac{x}{2} + (\frac{x}{2})^* \in H_0(K, *)$ for all $x \in H(K, *)$ and so $K_* = H_0(K, *) = H(K, *)$. If $\text{char} K = 2$, then $K_* \subset H_0(K, *) \subset H(K, *)$ is possible.

One has either $H_0(K, *) \subseteq Z(K)$ or $\langle H_0(K, *) \rangle = K$ as a ring ([19], (23.23)).

If K is a skewfield with involution $*$ and K_0 an ample hermitian Jordan algebra, then one calls $(K, K_0, *)$ an *involutory set*.

If L_0 is a K -vectorspace, then a map $\pi : L_0 \rightarrow K/K_0$ is called a *pseudo-quadratic form* relative to $(K, K_0, *)$ if $\pi(a\lambda) = \lambda^* \pi(a) \lambda$ for all $a \in L_0, \lambda \in K$ and if there is a skew-hermitian form $f : L_0 \times L_0 \rightarrow K$ relative to $*$ with $\pi(a+b) \equiv \pi(a) + \pi(b) + f(a, b) \pmod{K_0}$ for all $a, b \in L_0$. A subspace X_0 of L_0 is called *isotropic* if $\pi(a) = 0$ for all $a \in X_0$. The maximal dimension of an isotropic subspace is called the *Witt index* of π . If the Witt index is 0, then π is called *anisotropic*.

3 Cubic Action

From now on, we assume that $G = \langle A, B \rangle$ is a rank one group which acts cubically on a module V . Set $A_0 := C_A(V/C_V(A)) \cap C_A([V, A])$.

Proposition 3.1 (a) $A' \leq A_0 \leq Z(A)$.

(b) If $A_0 \neq 1$, then A_0 is a special root subgroup of A which acts quadratically on V .

Proof.

(a) The commutator map

$$[\cdot, \cdot]; V \times A \rightarrow V : (v, a) \mapsto [v, a] = -v + v^a$$

induces bilinear maps from $V/C_V(A) \times A$ to $[V, A]$ and from $[V, A] \times A$ to $[V, A, A]$. The right kernel of the first map is $C_A(V/C_V(A))$, the right kernel of the second map is $C_A([V, A])$. Both of these groups contain A' . Since A_0 is the intersection of these two groups, we get $A' \leq A_0$. If $a \in A_0, b \in A$, then $[v, a, b] = 0 = [v, b, a]$ and thus $[v, [b, a]] = 0$. Hence $[b, a] = 0$ and so $a \in Z(A)$.

(b) Let $a \in A_0^\#$, $\mu = \mu_a$, $B_0 = A_0^\mu = C_B([V, B]) \cap C_B(V/C_V(B))$ and $G_0 = \langle A_0, B_0 \rangle$. We have $[V, A_0] \subseteq C_V(A)$ and thus $[V, A_0, A] \subseteq [C_V(A), A] = 0$. Suppose that $[V, G, G_0] = 0$. Then $G_0 \leq C_G([V, G]) := N$. Since $A \cap N \neq 1$, we get $G = NA$. So $[V, G, G, G, G] = [V, G, A, A, A] = 0$. This implies that G is nilpotent, a contradiction. Thus A_0 is a special root subgroup of A by (2.4) of [16]. Since $[V, A_0, A] = 0$, we get $[V, A_0, A_0] = 0$. Thus A_0 acts quadratically on V .

□

We now present some examples.

Example 3.2 Suppose that $G = \langle A, B \rangle$ is a rank one group and that V is a quadratic module for G . If F is a subring of $\text{End}_G(V)$, then G acts on $\text{End}_F(V)$ by conjugation. We claim that this action is cubic. For $\varphi \in \text{End}_F(V), a \in A$ and $v \in [V, A]$ we have

$$v(-\varphi + a^{-1}\varphi a) = -v\varphi + v\varphi a = [v\varphi, a] \in [V, A],$$

so $[\text{End}_F(V), A] \subseteq \{\varphi \in \text{End}_F(V); [V, A]\varphi \subseteq [V, A]\}$. For $\varphi \in [\text{End}_F(V), A], v \in V$ we get

$$v(-\varphi + a^{-1}\varphi a) = -v\varphi + v\varphi a + [v, a^{-1}]\varphi a = [v\varphi, a] + [v, a^{-1}]\varphi \in [V, A].$$

If $v \in [V, A]$, then $v(-\varphi + a^{-1}\varphi a) = 0$. So we get $[\text{End}_F(V), A, A] \subseteq \{\varphi \in \text{End}_F(V); V\varphi \subseteq [V, A], [V, A]\varphi = 0\}$. With the formula above we obtain that $[\text{End}_F(V), A, A, A] = 0$. Since $G \subseteq \text{End}_F(V)$ and either G is perfect, $G \cong \text{SL}(2, 3)$ and $A = Z_3$, or $G \cong S_3$ and $A = Z_2$, we see that $[\text{End}_F(V), G, G, G] \neq$

0. If $G = SL_2(J, R)$ with $R = \langle J \rangle$, $V = R^2$ and A the group of lower unipotent triangle matrices with entries in J , then $C_A([End_F(V), A]) = A$ iff R is commutative and $char R = 2$ and $C_A([End_F(V), A]) = 1$ in all other cases. In all cases $A_0 = 1$.

Example 3.3 Let $(K, K_0, *)$ be an involutory set, \overline{V} a K -vectorspace and $\overline{\pi} : \overline{V} \rightarrow K/K_0$ an anisotropic pseudo-quadratic form with associated skew-hermitian form f . Define $V = K \oplus \overline{V} \oplus K$ and $\pi : V \rightarrow K/K_0$ by

$$\pi(r, x, s) = s^*r + \overline{\pi}(x) + K_0.$$

Then π is a pseudo-quadratic form with associated skew-hermitian form g given by

$$g((r, x, s), (t, y, u)) = u^*r - t^*s + f(x, y)$$

for $x, y \in \overline{V}$ and $r, s, t, u \in K$. We have $\pi(r, x, 0) \in K_0$ iff $x = 0$ and $\pi(r, x, 1) = 0$ iff $r + \overline{\pi}(x) \in K_0$. Thus $\{(1, 0, 0)K\} \cup \{(r, x, 1)K; r + \overline{\pi}(x) \in K_0\}$ is the set of anisotropic 1-dimensional spaces. Therefore the Witt index of π is 1. For $v \in \overline{V}, t \in K$ with $\pi(v) - t \in K_0$ let $\alpha_{(v,t)} \in End(V)$ be defined by

$$(r, x, s)\alpha_{(v,t)} = (r - f(v, x) + t^*s, x + vs, s)$$

for $x \in \overline{V}, r, s \in K$. Then $\alpha_{(v,t)} \in GL_K(V)$, $\alpha_{(v,t)}\alpha_{(w,u)} = \alpha_{(v+w, t+u+f(v,w))}$ and

$$\pi((r, x, s)\alpha_{(v,t)}) = \pi((r - f(v, x) + t^*s, x + vs, s)) =$$

$$s^*(r - f(v, x) + t^*s) + \overline{\pi}(v + xs) + K_0 =$$

$$s^*r + s^*f(x, v)^* + s^*t^*s + \overline{\pi}(v) + f(x, vs) + s^*\overline{\pi}(x)s + K_0 =$$

$$s^*r + \overline{\pi}(v) + s^*(t^* + t - (t - \overline{\pi}(v))s) + f(x, v)s + (f(x, v)s)^* + K_0 = \pi(r, x, s).$$

Similarly, define $\beta_{(t,v)}$ by

$$(r, x, s)\beta_{(t,v)} = (r, x - vr, s - f(v, x) - t^*r).$$

Then again $\pi((r, x, v)\beta_{(t,v)}) = \pi(r, x, v)$. If $A = \{\alpha_{(v,t)}; \overline{\pi}(v) - t \in K_0\}$ and $B = \{\beta_{(v,t)}; \overline{\pi}(v) - t \in K_0\}$, then $G = \langle A, B \rangle$ is an abstract rank one group and V is a cubic module for G . It is $[V, A] = \{(r, v, 0); r \in K, v \in V\}$ and $C_V(A) = \{(r, v, 0); r \in K, v \in rad(f)\}$. Therefore

$$A_0 = C_A([V, A]) = \{\alpha_{(v,t)}; v \in rad(f)\} = Z(A).$$

Example 3.4 We present one example with abelian root groups. Let K be a commutative field and let (L_0, q) be an anisotropic quadratic space over K with associated symmetric bilinear form f . Set $\overline{L}_0 = L_0/Def(q)$. For $v \in L_0$, \overline{v} denotes the image of v in \overline{L}_0 . Set $V = K \oplus \overline{L}_0 \oplus K$. For all $v \in L_0$ we define $\alpha_v, \beta_v \in GL(K, V)$ by

$$(x, \overline{w}, y)\alpha_v = (x, \overline{w} + \overline{v}x, y + f(\overline{w}, \overline{v}) + xq(v))$$

and

$$(x, \overline{w}, y)\beta_v = (x + f(\overline{w}, \overline{v}) + q(v)y, \overline{w} + \overline{v}y, y).$$

Then $\alpha_v\alpha_w = \alpha_{v+w}$ and $\beta_v\beta_w = \beta_{v+w}$ for all $v, w \in L_0$. Thus $A := \{\alpha_v; v \in L_0\}$ and $B := \{\beta_v; v \in L_0\}$ are groups isomorphic to L_0 . If $\text{Def}(q) = 0$ (which is always case if $\text{char}K \neq 2$), then $Q : V \rightarrow K : Q(x, \overline{w}, y) = xy - q(w)$ is a well-defined quadratic form of Witt index 1. Suppose $\text{Def}(q) \neq 0$. Then we may assume that there is an element $e \in \text{Def}(q)$ with $q(e) = 1$ (if not, we replace q by $q(e)^{-1}q$). Set $K_0 := q(\text{Def}(q))$. Then (K, K_0, id) is an involutory set. If we define $Q : V \rightarrow K/K_0$ by $Q(x, \overline{w}, y) = xy + q(w) + K_0$ (here w is a preimage of \overline{w} in L_0), then Q is a well-defined pseudo-quadratic form. In both cases, Q has Witt index 1 and the two groups A and B are contained in $O(Q) := \{\varphi \in GL(V, K); Q(z\varphi) = Q(z) \text{ for all } z \in V\}$. If $X = \{(0, 0, 1)K\} \cup \{(q(w), \overline{w}, 1)K; w \in L_0\}$, then X is the set of isotropic 1-dimensional subspaces of V . We write ∞ for $(1, 0, 0)K$ and v for $Kq(v), \overline{v}, 1)K$. One can see that A is the centralizer in $O(Q)$ of ∞ , V/∞^\perp and ∞^\perp/∞ . Similarly, B is the centralizer of 0 , $V/0^\perp$ and $0^\perp/0$. Thus $G = \langle A, B \rangle$ is a rank one group with unipotent subgroups A and B . Since $[V, A] \leq \infty^\perp$, $[\infty^\perp, A] \leq \infty$ and $[\infty, A] = 0$, V is a quadratic or cubic module for G . It is quadratic iff $V = \text{Def}(q)$. One can easily see that $A_0 = \{\alpha_v; v \in \text{Def}(q)\}$, so $A_0 \neq 1$ is only possible if $\text{char}K = 2$.

Example 3.5 If G is a Suzuki group or a Ree group, then there is no cubic module for G . In case of the Suzuki groups, this follows by the fact that every Suzuki group contains a Frobenius group of order 20 which has only one non-trivial irreducible module in characteristic 2 which is not cubic. If G is a Ree group, then there is an element $g \in G$ with $\text{o}(g) = 9$. So the minimal polynomial of g can not be $(X - 1)^3$ and g cannot act cubically.

Example 3.6 Let (L_0, q) be a quadratic space over a field K of type E_k with $k \in \{6, 7, 8\}$. Let $X_0, \cdot, \theta, h, g, \pi, \epsilon, Q$ as in Chapter 13 in [19]. Set $V = L_0 \oplus X_0 \oplus L_0$. For $a \in X_0, t \in K$ and $(u, x, v) \in V$ let $\alpha_{(a,t)} \in GL(V)$ be given by

$$(u, x, v)\alpha_{(a,t)} = (u, x + a \cdot u, v + \theta(a, u) + h(a, x) + tu).$$

Then we have

$$\begin{aligned} (u, x, v)\alpha_{(a,t)}\alpha_{(b,s)} &= (u, x + a \cdot u, v + \theta(a, u) + h(a, x) + tu)\alpha_{(b,s)} = \\ (u, x + a \cdot u + b \cdot u, v + \theta(a, u) + h(a, x) + tu + \theta(b, u) + h(b, x) + h(b, a \cdot u) + su) &= \\ (u, x + (a+b) \cdot u, v + \theta(a+b, u) + h(a+b, x) + (s+t+g(a, b))u) &= (u, x, v)\alpha_{(a+b, s+t+g(a, b))} \end{aligned}$$

by (13.37) in [19]. Thus $A = \{\alpha_{(a,t)}; a \in X_0, t \in K\}$ is isomorphic to the group S in (16.6) of [19]. Let $\tau \in GL(V)$ be given by $(u, x, v)\tau = (-v, x, u)$ and set $G = \langle A, \tau \rangle$. Set $M_\infty := \{(0, 0, v); v \in L_0\}$, $M_0 = M_\infty\tau = \{(u, 0, 0); u \in L_0\}$ and $M_{(a,t)} := M_0\alpha_{(a,t)} = \{(u, a \cdot u, \theta(a, u) + tu); u \in L_0\}$ for $a \in X_0, t \in K$. We claim that if $(a, t) \neq (0, 0)$, then $M_{(a,t)}\tau^{-1} = M_{(b,s)}$ with

$$b = \frac{1}{q(\pi(a) + t\epsilon)}(a \cdot \overline{\pi(a)} + ta) \text{ and } s = -\frac{1}{q(\pi(a) + t\epsilon)}(t + Q(a)).$$

All citations will refer to [19]. We have

$$b \cdot (\theta(a, v) + tv) = b \cdot \theta(a, v) + tb \cdot v =$$

$$\frac{1}{q(\pi(a) + t\epsilon)}(a\overline{\pi(a)}\theta(a, v) + ta\theta(a, v) + ta \cdot \overline{\pi(a)}v + t^2a \cdot v).$$

By (13.39) and (13.56) (ii) we get

$$b \cdot (\theta(a, v) + tv) = \frac{1}{q(\pi(a) + t\epsilon)}(q(\pi(a))a \cdot v + ta \cdot (\pi(a) + \overline{\pi(a)}) \cdot v + t^2a \cdot v) =$$

$$\frac{1}{q(\pi(a) + t\epsilon)}a \cdot (q(\pi(a)) + f(\pi(a), t\epsilon) + q(t\epsilon))v = \frac{1}{q(\pi(a) + t\epsilon)}a \cdot q(\pi(a) + t\epsilon)v = a \cdot v.$$

By (13.42) we have $a \cdot \overline{\pi(a)} = a \cdot (-\pi(a) + Q(a)\epsilon) = -a \cdot \pi(a) + Q(a)a$. By (13.35) and (13.37) we have

$$\theta(b, w) =$$

$$\frac{1}{q(\pi(a) + t\epsilon)^2}(\theta(a\pi(a), w) + (t + Q(a))^2\theta(a, w) - (t + Q(a))(h(a, a\pi(a)w) - g(a\pi(a), a)w))$$

for $w \in L_0$. With (a) and (b) in the proof of (13.67) we get

$$\theta(b, w) = \frac{1}{q(\pi(a) + t\epsilon)^2}(q(\pi(a))\theta(a, w) + (t + Q(a))^2\theta(a, w) - (t + Q(a))Q(a)\theta(a, w)) =$$

$$\frac{1}{q(\pi(a) + t\epsilon)^2}(q(\pi(a)) + tQ(a) + t^2)\theta(a, w) = \frac{1}{q(\pi(a) + t\epsilon)^2}q(\pi(a) + t\epsilon)\theta(a, w)$$

$$= \frac{1}{q(\pi(a) + t\epsilon)}\theta(a, w).$$

For $w = \theta(a, v) + tv$ we get with (13.28), (13.34) and (13.56) (iii)

$$\theta(b, \theta(a, v) + tv) = \frac{1}{q(\pi(a) + t\epsilon)}\theta(a, \theta(a, v) + tv) = \frac{1}{q(\pi(a) + t\epsilon)}(\theta(a, \theta(a, v)) + t\theta(a, v))$$

$$= \frac{1}{q(\pi(a) + t\epsilon)}((Q(a)\theta(a, v) - q(\pi(a))v + t\theta(a, v)).$$

Hence we get

$$\theta(b, \theta(a, v) + tv) + s(\theta(a, v) + tv) =$$

$$\frac{1}{q(\pi(a) + t\epsilon)}((Q(a) + t)\theta(a, v) - q(\pi(a))v - (t + Q(a))(\theta(a, v) + tv)) =$$

$$-\frac{1}{q(\pi(a) + t\epsilon)}(q(\pi(a)) + tQ(a) + t^2)v = -\frac{1}{q(\pi(a) + t\epsilon)}q(\pi(a) + t\epsilon)v = -v.$$

Thus we get

$$M_{(b,s)} = \{(\theta(a, v) + tv, a \cdot v, -v); v \in L_0\} = M_{(a,t)}\tau^{-1}.$$

With (32.10) in [19] one sees that $X := \{M_\infty\} \cup \{M_{(a,t)}; a \in X_0, t \in K\}$ is a Moufang set with root groups isomorphic to A . Let N be the kernel of the action of G on X and set $B := A^\tau$.

If $\phi \in N$, then ϕ leaves M_0 and M_∞ invariant, thus there are $\psi_1, \psi_2 \in GL(L_0)$ with $(u, 0, 0)\phi = (u\psi_1, 0, 0)$ and $(0, 0, v)\phi = (0, 0, v\psi_2)$ for all $u, v \in L_0$. Since ϕ fixes $M_{(0,1)}$, we get for all $u \in L_0$ that $(u, 0, u)\phi = (u, 0, 0)\phi + (0, 0, u)\phi = (u\psi_1, 0, 0) + (0, 0, u\psi_2) = (u\psi_1, 0, u\psi_2) \in M_1$. Hence $\psi_1 = \psi_2 = \psi$. Set $A_0 := \{\alpha_{(0,t)}; t \in K\}$. If $C_{NA_0}(V/M_\infty) > A_0$, then there would be a $1 \neq \phi \in C_N(V/M_\infty)$. Since ϕ stabilizes M_0 , ϕ centralizes M_0 and thus also M_∞ . If $v \in L_0, a \in X_0, t \in K$, then there is a $u \in L_0$ with $(v, a \cdot v, tv + \theta(a, v))\phi = (v, a \cdot v, u)$. But $(v, a \cdot v, tv + \theta(a, v))\phi \in M_{(a,t)}$ and hence $(v, a \cdot v, tv + \theta(a, v))\phi = (v, a \cdot v, tv + \theta(a, v))$. If $a \in X_0$, then ϕ centralizes $(\epsilon, 0, 0), (0, 0, \theta(a, \epsilon))$ and $(\epsilon, a, \theta(a, \epsilon))$. Hence ϕ centralizes $(0, a, 0)$ and thus $\phi = 1$. We conclude that $A_0 = C_{NA_0}(V/M_\infty)$. This implies that N and A_0 centralize each other. Therefore N stabilizes $C_V(A_0) := \{(0, x, v); x \in X_0, v \in L_0\}$. We conclude that $A \leq C_{NA}(V/C_V(A_0))$. If equality doesn't hold, then again there is $1 \neq \phi \in C_N(V/C_V(A_0))$. We see again that ϕ centralizes M_0 and M_∞ . If $v \in L_0, a \in X_0, t \in K$, then there are $b \in X_0, v \in L_0$ with $(v, a \cdot v, tv + \theta(a, v))\phi = (v, b, u)$. But $(v, a \cdot v, tv + \theta(a, v))\phi \in M_{(a,t)}$ and thus again $(v, a \cdot v, tv + \theta(a, v))\phi = (v, a \cdot v, tv + \theta(a, v))$. Again we may conclude that $\phi = 1$. It follows that $A = C_{NA}(V/C_V(A_0))$.

If $a \in A^\#$, then there is a unique $b \in B^\#$ with $(AN)^b = (BN)^a$, thus $B^{ab^{-1}} \leq AN$. If $B_0 = A_0^\tau$, then $B_0 = C_{NB}(V/V_0)$ and thus $B_0^{ab^{-1}} = C_{NA}(V/V_\infty) = A_0$. Moreover $B = C_{NB}(V/C_V(B_0))$ and thus $B^{ab^{-1}} = C_{NA}(V/C_V(A_0)) = A$. This shows that G is a rank one group with unipotent subgroups A and B .

Example 3.7 Suppose that k is a field of odd characteristic, M a finite-dimensional k -vectorspace and $G \leq GL_K(M)$ which satisfies hypothesis (H) in [18], hence

- (a) $M = [M, G]$.
- (b) G is generated by a set Σ of subgroups of G such that $[M, A, A] = 0$ for all $A \in \Sigma$ and $\langle A, B \rangle$ is a rank one group.
- (c) If $\sigma \in G$ is a quadratic element, then σ is contained in an element of G iff with $\dim[M, \sigma]$ is minimal.

For $A \in \Sigma$ we set

$$U(A) := \{\varphi \in G; [M, \varphi] \subseteq C_M(A), [C_M(A), \varphi] \subseteq [M, A] \text{ and } [M, A, \varphi] = 0\}.$$

Then $[M, U(A), U(A), U(A)] = 0$. If $A, B \in \Sigma$ with $A \neq B$, then by Proposition 1 in [18] we have that $G = \langle U(A), U(B) \rangle$ and G is a rank one group with unipotent subgroups $U(A)$ and $U(B)$. By definition, M is a cubic module for G . By (c) of 3.11 one sees that $U(A)_0 = A$ for all $A \in \Sigma$ holds.

From now on, we assume that $G = \langle A, B \rangle$ acts cubically on a $\mathbb{Z}G$ -module V . We assume further that $A_0 := C_A([V, A]) \cap C_A(V/C_V(A)) \neq 1$. Set $G := \langle A_0, B_0 \rangle$ and $H_0 := N_{G_0}(A_0) \cap N_{G_0}(B_0)$.

Lemma 3.8 (a) Set $V_0 = V$, $V_{i+1} = [V_i, G]$ and $W = \bigcap_{i \geq 0} V_i$. Then W is a cubic module for G with $W = [W, G]$.

(b) Set $Z_0 = C_V(G)$, let Z_{i+1} be the preimage of $C_{V/Z_i}(G)$ in V and set $Z = \bigcup_{i \geq 0} Z_i$. Then V/Z is a cubic module for G with $C_{V/Z}(G) = 0$.

Proof. Suppose first $|A_0| > 3$. Then G_0 is perfect (1.1 in [16]). Thus $[V, G_0] = [V, G_0, G_0]$ and so $0 \neq [V, G_0] \leq W$. If $[W, G, G, G]$ would be 0, then also $[V, G_0, G_0, G_0] = 0$, which would imply $[V, G_0] = 0$, a contradiction. Moreover, $Z_i \leq C_V(G_0)$ for all $i \geq 0$ and thus $Z \leq C_V(G_0) \neq V$. If $[V/Z, G, G, G]$ would be zero, then also $[V/C_V(G_0), G_0, G_0, G_0] = 0$, a contradiction.

Suppose A_0 has order 2 or 3. Then again by Theorem 1.1. in [16] either $G_0 \cong S_3$ or $G \cong SL_2(3)$. In the first case let t be a generator of $G'_0 \cong A_3$, in the second let t be the central involution in G_0 . In both cases we have $V = C_V(t) \oplus [V, t]$. Thus $0 \neq [V, t] = [V, t, t]$ and so $0 \neq [V, t] \leq W$. Again, $[W, G_0, G_0, G_0] = 0$ implies $0 = [W, t, t, t] = [W, t, t] = [W, t]$, a contradiction. Moreover, we have again $Z \leq C_V(t) \neq V$. If $[V/Z, G, G, G] = 0$ would hold, then again $[V/C_V(t), t, t, t] = 0$, a contradiction. \square

From now on we will assume that $[V, G] = V$ and $C_V(G) = 0$.

Lemma 3.9 If V is a cubic module for G with $[V, G] = V$ and $A_0 \neq 1$, then V, A_0 and A/A_0 are either elementary abelian p -groups for a prime p or V and A_0 are torsion free and unique divisible and A/A_0 is torsion free.

Proof. Since $[V, G] = V$, we have $[V/W, G] = V/G$ for every G -submodule W of V . This implies that either $V = W$ or V/W is a cubic module for G . Suppose there is a prime p such that $pV \neq V$. Then V/pV is a cubic module for G . This implies that A has exponent at most p^2 . Thus $qV = V$ for all primes $q \neq p$. Since A_0 acts quadratically on V , A_0 has exponent p , and since the commutator map from $V \times A_0$ to $C_V(A)$ is bilinear, we get $[V, A_0] \subseteq V_p := \{v \in V; pv = 0\}$. Therefore A_0 acts trivial on V/V_p , so the action of G on V/V_p cannot be cubic. Thus $V = V_p$ and so $pV = 0$. Now the commutator map induces biadditive map from $A/C_A([V, A]) \times [V, A]$ to $[V, A]$ and from $A/C_A(V/C_V(A)) \times V/C_V(A)$ to $V/C_V(A)$. This shows that $A/C_A([V, A])$ and $A/C_A(V/C_V(A))$ are elementary-abelian p -groups. Thus A/A_0 is an elementary-abelian p -group.

If $pV = V$ for all primes p , then $V = nV$ for all natural numbers n , so V is uniquely divisible.

Since the commutator map induces a bilinear map from $V \times A_0$ to V , one sees that A_0 is of exponent p iff V is. If V is torsion-free, then so is A_0 . By 1.1 in [16] we get that A_0 is uniquely divisible. If $a \in A$ and $n \geq 1$ with $a^n \in A_0$, then $n[v, a] = 0$ for all $v \in [V, A]$ and $n[w, a] \in C_V(A)$ for all $w \in V$. This implies $a \in A_0$ and so A/A_0 is torsion free. \square

We therefore can define a characteristic on V and A which is p if V is an

elementary p -group and which is 0 if V is torsion-free and uniquely divisible. We will later see that if $\text{char} V = 0$, then also A/A_0 is uniquely divisible (see 4.12).

Example 3.4 shows that it is possible that A is abelian and $A_0 \neq 1$. The next lemma shows that this can only happen if the characteristic of V is 2.

Proposition 3.10 *If A is abelian and $A_0 \neq 1$, then A is an elementary-abelian 2-group.*

Proof. Since A is abelian, the corresponding Moufang set is by [12] either special or non-proper (and thus $G/Z(G)$ is a sharply 2-transitive permutation group). If G is special, then the claim follows by [14]. So we have to show that the last case cannot hold.

Suppose that $G/Z(G)$ is sharply 2-transitive. Then also the Moufang set corresponding to G_0 is non-proper. By [2], 11.48 there is a commutative field K with $A \cong K^*$. By I(2.5) and (3.1) in [16], G_0 is a special rank one group. By [4] 4.9 (4) the order of A_0 is at most 3. So V is an elementary abelian p -group with $p = 2$ or $p = 3$. If $p = 2$, then the exponent of A is at most 4 since the minimal polynomial of every element of A divides $(X - 1)^3$ and thus $(X - 1)^4 = X^4 - 1$. Thus A is cyclic of order 2 or 4. In the first case $A \cong \mathbb{F}_3^* \cong A_0$, a contradiction, in the second case G is the Frobenius group of order 20. But this group doesn't act cubically on a module of characteristic 2.

Suppose $p = 3$. Since the minimal polynomial of every element of A divides $(X - 1)^3 = X^3 - 1$, A is elementary-abelian of order 3. Since $A \cong K^*$ for a field K , we get $A \cong \mathbb{F}_4^* \cong A_0$, a contradiction. \square

If $G = \langle A, B \rangle$ is a rank one group which acts quadratically on a module V , then $[V, G] = V$ and $C_V(G) = 0$ implies $V = [V, A] \oplus [V, B] = C_V(A) \oplus C_V(B)$ (see 2.1 (8) of [17]). In the cubic case, there is a similar decomposition of V .

Lemma 3.11 (a) $V = C_V(A) \oplus [V, B]$.

(b) $C_V(A) = [V, A_0] = [V, a]$ for all $a \in A_0^\#$.

(c) $[V, A] = C_V(a)$ for all $a \in A_0^\#$.

(d) If A is not abelian, then $C_V(A) = [V, A, A]$.

Proof.

- (a) Set $W := C_V(A) + [V, B]$. Then both A_0 and B operate trivially on V/W . Since $G = \langle A_0, B \rangle$, we get $V = [V, G] \leq W$. Similarly, both A and B_0 operate trivially on $[V, B] \cap C_V(A)$ and thus $G = \langle A, B_0 \rangle \leq C_G([V, B] \cap C_V(A))$. Thus we get $[V, B] \cap C_V(A) \leq C_V(G) = 0$. Hence V is the direct sum of $C_V(A)$ and $[V, B]$.

- (b) If $a \in A_0^\#$, then $[V, a] \leq C_V(A)$. Since $G = \langle B, a \rangle$, the equation $V = [V, a] + [V, B]$ follows with the same argument as in (a). Thus $[V, a] = C_V(A)$. Since $[V, A_0] \leq C_V(A) = [V, a] \leq [V, A_0]$, the remaining equation follows.
- (c) If $a \in A_0^\#$, then by definition $[V, A] \leq C_V(a)$. Suppose there is a $v \in C_V(a) \setminus [V, A]$. Now (a) implies $V = [V, A] \oplus C_V(B)$ and thus we get $W := C_V(B) \cap C_V(a) \neq 0$. But then $G = \langle B, a \rangle \leq C_G(W)$, a contradiction.
- (d) Since A acts quadratically on $V/[V, A, A]$, we get $1 \neq A' \leq C_A(A/[V, A, A])$ and thus $[V, A'] \leq [V, A, A]$. But since $A' \neq 1$, we get $C_V(A) = [V, A'] \leq [V, A, A]$ by (b). Since $[V, A, A, A] = 0$, we also have $[V, A, A] \leq C_V(A)$ and thus equality holds.

□

Lemma 3.12 (a) $[V, A] \cap [V, B] = C_V(G_0)$.

(b) $[V, A] = C_V(A) \oplus C_V(G_0)$.

Proof.

- (a) Since $G_0 = \langle A_0, B_0 \rangle$, we get $C_V(G_0) = C_V(A_0) \cap C_V(B_0) = [V, A] \cap [V, B]$.
- (b) Set $V_0 = [V, A_0] + [V, B_0]$. Then $V_0 = [V, G_0]$. Suppose first $\text{char} V \neq 2$. By 4.2 (a) in [17], [14] we get $V = C_V(G_0) \oplus V_0$. Thus we have

$$[V, A] \oplus C_V(B) = V = C_V(G_0) \oplus C_V(A) \oplus C_V(B).$$

Since $C_V(A) \oplus C_V(G_0) \leq [V, A]$, equality must hold.

Now suppose $\text{char} V = 2$. If $a \in A_0^\#$ and $b = b(a)$, then $t := ab$ has order 3. If $v \in C_V(t)$, then $v + [v, a] = va = vb = v + [v, b]$ and thus

$$[v, a] = [v, b] \in [V, A_0] \cap [V, B_0] = 0.$$

Thus $C_V(t) = C_V(a) \cap C_V(b) = C_V(G_0)$. Since $V = [V, t] \oplus C_V(t)$ and $[V, t] \leq V_0$ we again get $V = V_0 \oplus C_V(G_0)$.

□

4 The structure of G_0

We will fix the following notation. Let $0 \neq e \in A_0$ be fixed and set $\mu = \mu_{e^{-1}}$. If A has characteristic 2 and A is not abelian, we choose e in such a way that $e = a^2$ for an element $a \in A$. For $a \in A_0^\#$ set $h_a := \mu\mu_a$ and $h_1 = 0$. Let $\rho : H \cup \{h_1\} \rightarrow \text{End}(C_V(A)) : h \mapsto h|_{C_V(A)}$.

Lemma 4.1 If $v \in C_V(A)$ and $a \in A^\#$, then $vh_a = v\mu + [v\mu, a] + [v\mu, a, b(a)^{-1}]$.

Proof. We have by definition $h_a = \mu b(a^{-1})ab(a)^{-1}$ and thus

$$vh_a = v\mu b(a^{-1})ab(a)^{-1} = v\mu ab(a)^{-1},$$

since $v\mu \in C_V(A)^\mu = C_V(B)$. Thus

$$vh_a = (v\mu + [v\mu, a])b(a)^{-1} = v\mu + [v\mu, a] + [v\mu, a, b(a)^{-1}].$$

□

Corollary 4.2 (a) $vh_a - [v\mu, a] = v\mu + [v\mu, a, b(a)^{-1}] \in C_V(G_0)$.

(b) If $a \in A_0$, then $vh_a = [v\mu, a]$.

(c) $\rho(h_{ab}) = \rho(h_a) + \rho(h_b)$ for all $a, b \in A_0$.

Proof.

- (a) By 4.1 $vh_a - [v\mu, a] = v\mu + [v\mu, a, b(a)^{-1}] \in [V, A] \cap [V, B] = C_V(G_0)$.
- (b) If $a \in A_0^\#$, then $vh_a - [v\mu, a] \in [V, A_0] \cap [V, B_0] = 0$. For $a = 1$, $vh_1 = 0 = [v\mu, 1]$.
- (c) For $v \in C_V(A)$, $a, b \in A_0$ we have $v\rho(h_{ab}) = vh_{ab} = [v, ab] = [v, a] + [v, b] = vh_a + vh_b = v\rho(h_a) + v\rho(h_b)$ and thus $\rho(h_{ab}) = \rho(h_a) + \rho(h_b)$.

□

By 3.7 in [17], we get that $J := \{\rho(h_a); a \in A_0\}$ is a special quadratic Jordan division algebra in $End(C_V(A))$. Let R be the subring of $End(C_V(A))$ generated by J and S the subring of $End(C_V(A))$ generated by $\rho(H)$. Notice that R is generated by $\rho(H_0)$. Since $\rho(\mu^2) = -1$ ([17], 3.2), for all $r \in R$ there are elements $h_i \in H_0$ with $r = \sum_i \rho(h_i)$.

Proposition 4.3 Set $f : A \times A \rightarrow End(C_V(A)) : (a, b) \mapsto (v \mapsto [v\mu, a, b])$. Then:

- (a) f is biadditive.
- (b) $f(a, b^h) = f(a, b)\rho(h)$ and $f(a^h, b) = \rho(h^{-\mu})f(a, b)$ for all $a, b \in A$ and all $h \in H_0$.
- (c) $C_A(V/C_V(A))$ is the left kernel of f and $C_A([V, A])$ is the right kernel of f .
- (d) $f(a, b) - f(b, a) = \rho(h_{[a, b]})$ for all $a, b \in A$.
- (e) If the characteristic of A is 2, then $f(a, a) = \rho(h_{a^2})$.

Proof.

- (a) Let $a, b, c \in A$. Then we have $(a-1)(b-1)(c-1) = 0$ in $End(V)$. Thus we get $(ab+1)(c-1) = (a+b)(c-1)$ and hence $(ab-1)(c-1) = (a+b-2)(c-1)$. It follows

$$vf(ab, c) = v\mu(ab-1)(c-1) = v\mu(a+b-2)(c-1) =$$

$$v\mu(a-1)(c-1) + v\mu(b-1)(c-1) = vf(a, c) + vf(b, c)$$

for all $v \in C_V(A)$. We also get $(a-1)(bc+1) = (a-1)(b+c)$ and thus $(a-1)(bc-1) = (a-1)(b-1) + (a-1)(c-1)$. This implies

$$vf(a, bc) = v\mu(a-1)(bc-1) = v\mu(a-1)(b-1) + v\mu(a-1)(c-1) = vf(a, b) + vf(a, c)$$

for all $v \in V$. Therefore f is biadditive.

(b) We first claim that

$$v\mu(a-1)h(b-1) = vf(a, b)$$

for all $a, b \in A$, all $v \in C_V(A)$ and all $h \in H_0$ holds. We have $v\mu(a-1) = [v\mu, a] = [v\mu, a] - vh_a + vh_a$. Since $[v\mu, a] - vh_a \in C_V(G_0)$, we get

$$v\mu(a-1)h = [v\mu, a] - vh_a + vh_a h$$

and thus

$$v\mu(a-1)h(b-1) = [v\mu, a](b-1) + (vh_a h - vh_a)(b-1) = [v\mu, a, b] = vf(a, b),$$

since $vh_a h - vh_a \in C_V(A) = C_V(A)$.

We now get

$$vf(a, b^h) = v\mu(a-1)(b^h-1) = v\mu(a-1)h^{-1}(b-1)h = vf(a, b)h = vf(a, b)\rho(h)$$

and

$$\begin{aligned} vf(a^h, b) &= v\mu(a^h-1)(b-1) = v\mu h^{-1}(a-1)h(b-1) = vh^{-\mu^{-1}}\mu(a-1)h(b-1) \\ &= v\rho(h^{-\mu})\mu f(a, b), \end{aligned}$$

since $\mu^2 \in Z(G_0)$ ([17], 3.2).

(c) Suppose that $a \in A$. Then $f(a, b) = 0$ for all $b \in A$ iff $[v\mu, a] \in C_V(A) = C_V(A)$ for all $v \in C_V(A)$. Therefore $f(a, b) = 0$ for all $b \in A$ iff $[C_V(B), a] \subseteq C_V(A)$. Since $V = [V, A] \oplus C_V(B)$ and $[[V, A], a] \subseteq [V, A, A] \leq C_V(A)$ by definition, this holds iff $[V, a] \subseteq C_V(A)$ and thus iff $a \in C_A(V/C_V(A))$.

Similarly, $f(b, a) = 0$ for all $b \in A$ holds iff $[C_V(B), A] \subseteq C_V(a)$. Since $V = C_V(B) \oplus [V, A]$ and $[[V, A], A] \subseteq C_V(a)$, this holds iff $[V, A] \subseteq C_V(a)$ and thus iff $a \in C_A([V, A])$.

(d)

$$vf(a, b) - vf(b, a) = v\mu(a-1)(b-1) - v\mu(b-1)(a-1) = v\mu(ab - ba) =$$

$$v\mu ba(a^{-1}b^{-1}ab - 1) = v\mu ba([a, b] - 1) = v\mu([a, b] - 1)ba =$$

$$[v\mu, [a, b]]ba = [v\mu, [a, b]],$$

since $[a, b] \in A' \subseteq A_0 \subseteq Z(A)$ and $[v\mu, [a, b]] \in [V, A_0] = C_V(A)$. Thus the claim follows.

(e) $v\mu f(a, a) = v\mu(a-1)^2 = v\mu(a^2 - 1) = [v\mu, a^2] = v\rho(h_{a^2})$ for all $a \in A$ and all $v \in C_V(A)$.

□

Set $\overline{A} = A/A_0$ and $\overline{a} := A_0a$ for $a \in A$. By the previous proposition, we can regard f as a biadditive map from $\overline{A} \times \overline{A}$ to $\text{End}(C_V(A))$. We will use the additive notation for \overline{A} , so $\overline{a} + \overline{b}$ means A_0ab for $a, b \in A$ and $\overline{0}$ means the neutral element in \overline{A} .

The map f is linked to the map $a \mapsto \rho(h_a)$ from A to S .

Proposition 4.4 $f(a, b) = \rho(h_{ab}) - \rho(h_a) - \rho(h_b)$ for all $a, b \in A$.

Proof. For $v \in C_V(A)$ we have

$$vh_{ab} - [v\mu, ab] - (vh_a - [v\mu, a]) - (vh_b - [v\mu, b]) \in C_V(G_0).$$

Thus

$$\begin{aligned} v\rho(h_{ab}) - v\rho(h_a) - v\rho(h_b) - v\mu(ab - 1) + v\mu(a - 1) + v\mu(b - 1) = \\ v\rho(h_{ab}) - v\rho(h_a) - v\rho(h_b) - v\mu(ab - a - b + 1) = \\ v\rho(h_{ab}) - v\rho(h_a) - v\rho(h_b) - vf(a, b) \in C_V(G_0). \end{aligned}$$

But we also have $v\rho(h_{ab}) - v\rho(h_a) - v\rho(h_b) - vf(a, b) \in C_V(A)$. Since $C_V(A) \cap C_V(G_0) = 0$, the claim follows. \square

We immediately get

Corollary 4.5 $f(a, b) \in S$ for all $a, b \in A$.

The next lemma might be useful for an inductive approach.

Proposition 4.6 (a) $C_A(v)$ is a root subgroup of A for all $v \in C_V(G_0)$.

(b) If W is a subgroup of $C_V(G_0)$, then $C_A(V/(W + C_V(A)))$ is a root subgroup of A .

Proof.

(a) If $a \in C_A(v)$, $b = b(a)^{-1}$ and $a' = a(b)^{-1}$, then $h = \mu aba' \in H$. Thus $vh = v\mu aba' = vba' = (v + [v, b])a' \in C_V(G_0) \leq [V, A]$ and so $v + [v, b] \in [V, A]$ and $[v, b] \in [V, A]$. But $v \in C_V(G_0) \leq [V, B]$ and so $[v, b] \in [V, A] \cap C_V(B) = 0$. It follows $b \in C_B(v)$. Similarly, one can show that if $b \in C_B(v)$, then $a(b) \in C_A(v)$. Thus the claim follows.

(b) Let $v \in C_V(A)$ and $a \in C_A(V/(C_V(A) + W))$. Let b, a' and h as in (a). Then

$$vh = v\mu aba' = (v\mu + [v\mu, a])ba' = (v\mu + [v\mu, a] + [v\mu, a, b])a'.$$

Since $vh \in C_V(A)$, this implies

$$vh = v\mu + [v\mu, a] + [v\mu, a, b]$$

and so

$$vh - [v\mu, a] = v\mu + [v\mu, a, b] \in [V, A] \cap [V, B] = C_V(G_0).$$

Now $vh - [v\mu, a] \in C_V(G_0) \cap (C_V(A) + W) = W$. Thus $v\mu - [v\mu, a, b] \in W$. Now $v\mu - [v\mu, a, b] = v\mu - [[v\mu, a] - vh_a, b] - [vh_a, b]$ and so $[vh_a, b] \in W + C_V(B)$ since $v\mu - [[v\mu, a] - vh_a, b] \in C_V(B)$. This implies $[C_V(A), b] \subseteq W + C_V(B)$. Since $V = C_V(A) \oplus [V, B]$ and $[[V, B], b] \subseteq [V, B, B] \subseteq C_V(B)$ it follows that $b \in C_B(V/(C_V(B) + W))$. A similar argument shows that if $b \in C_B(V/(W + C_V(B)))$, then $a(b) \in C_A(V/(W + C_V(A)))$. Thus the claim follows. \square

The map $h \mapsto h^{-\mu}$ of H will later be needed to define an anti-automorphism on R .

Lemma 4.7 (a) $\rho(h_a^{-\mu}) = -\rho(h_{a^{-1}})$ for all $a \in A$.

(b) $\rho(h_a^{-\mu}) = \rho(h_a)$ for all $a \in A_0$.

(c) $h_{a^h} = h^{-\mu} h_a h$ for all $h \in H, a \in A$.

(d) $h^{-\mu} h \in H_0$ for all $h \in H$.

Proof.

(a) We have $h_a^{-\mu} = \mu^{-1} h_a^{-1} \mu = \mu^{-1} \mu_a^{-1} \mu^{-1} \mu = \mu^{-2} h_a$. Now $\rho(\mu^{-2}) = -1$ by 3.2 in [17]. Thus the claim follows.

(b) If $a \in A_0$, then $-\rho(h_a) = \rho(h_{a^{-1}})$ by 4.2(b). Thus the claim follows.

(c) We have $\mu_{a^h} = \mu_a^h = h^{-1} \mu_a h$ and thus $h_{a^h} = \mu h^{-1} \mu_a h = h^{-\mu^{-1}} \mu \mu_a h = h^{-\mu^{-1}} h_a h$. Now μ^2 inverts every element in $C_V(A) + C_V(B)$ and fixes every element in $C_V(G_0)$. Since h stabilizes these two subspaces, we have $[\mu^2, h] = 1$ and thus $h^{-\mu} = h^{-\mu^{-1}}$.

(d) This follows by (c) with $a = e$. \square

Lemma 4.8 For all $b \in A$, both $\rho(h_b)$ and $\rho(h_b) + 1$ normalize R .

Proof. For $b \in A, a \in A_0$ we have by 4.7

$$\rho(h_b)^{-1} \rho(h_a) \rho(h_b) = \rho(h_b^{-1}) \rho(h_b^\mu) \rho(h_b^{-\mu}) \rho(h_a) \rho(h_b) = \rho(h_{eh_b^\mu}) \rho(h_{ah_b}) \in R$$

and

$$\rho(h_b) \rho(h_a) \rho(h_b)^{-1} = \rho(h_b) \rho(h_b^{-\mu}) \rho(h_b^\mu) \rho(h_a) \rho(h_b^{-1}) = \rho(h_{eh_b^{-\mu}}) \rho(h_{ah_b^{-1}}) \in R.$$

Thus $\rho(h_b)$ normalizes R . This also holds for $\rho(h_{be}) = \rho(h_b) + 1$. \square

Proposition 4.9 *Suppose that R has only finitely many maximal ideals and that if $x \in R$ has an inverse in S , then $x^{-1} \in S$. If J is not commutative, then $R = S$.*

Proof. Let $Z(J) := \{x \in J; x + \mathfrak{B}(R) \in Z(R/\mathfrak{B}(R))\}$. If M is a maximal ideal of R and $x \in J$ with $x + M \in Z(R/M)$, then $[x, y]^2, [x, y, z] \in M \cap J = 0$. Thus $[x, y]$ is nilpotent, and since $J \subseteq C_R([x, y])$, we get $[x, y] \in Z(R)$. Therefore $[x, y] \in \mathfrak{B}(R)$ and so $x + \mathfrak{B}(R) \in Z(R/\mathfrak{B}(R))$. Therefore the preimage of $Z(R/M)$ in J is just $Z(J)$ and doesn't depend on M . Note that $J/Z(J)$ is either a vectorspace over \mathbb{Q} or a infinite-dimensional \mathbb{F}_p -vectorspace. Therefore $J/Z(J)$, regarded as additive group, contains infinitely many cyclic subgroups.

Suppose that $b \in A$ with $\rho(h_b) \notin R$. Then $\rho(h_b)^{-1} \notin R$ and $\rho(h_{ba}) \notin R$ for all $a \in A_0$. Since $J/Z(J)$ contains infinitely many cyclic subgroups, there are $a, c \in A_0$ and a maximal ideal M of R such that $I_{\rho(h_{ba})}, I_{\rho(h_{bc})} \subseteq M$ and such that $\rho(h_a), \rho(h_c)$ are not in $Z(J)$ and the groups generated by $\rho(h_a)$ and $\rho(h_c)$ in $J/Z(J)$ are distinct. Thus also $\rho(h_{ac^{-1}}) \notin Z(J)$. By replacing $\rho(h_b)$ through $\rho(h_{bc})$ and a by $c^{-1}a$, we may assume $I_{\rho(h_b)}, I_{\rho(h_{ba})} \subseteq M$ and $\rho(h_a) \notin Z(J)$. Therefore

$$u - (\rho(h_b) - 1)^{-1}u(\rho(h_b) - 1), u - (\rho(h_{ba}) - 1)^{-1}u(\rho(h_{ba}) - 1) \in M$$

for all $u \in R$. We get

$$\rho(h_b)u - u\rho(h_b) = -u + \rho(h_b)u - u\rho(h_b) + u =$$

$$(\rho(h_b) - 1)u - u(\rho(h_b) - 1) \in (\rho(h_b) - 1)M \subseteq \rho(h_b)M + M$$

and similarly

$$u\rho(h_b) + u\rho(h_a) - \rho(h_b)u - \rho(h_a)u = (\rho(h_{ba}) - 1)u - u(\rho(h_{ba}) - 1)$$

$$\in (\rho(h_{ba}) - 1)M \subseteq \rho(h_b)M + (\rho(h_a) - 1)M = \rho(h_b)M + M.$$

Thus we get

$$u\rho(h_a) - \rho(h_a)u \in (\rho(h_b)M + M) \cap R =: J_b.$$

We see immediately that J_b is a right ideal of R . Moreover, for all $u, v \in M$ and all $s \in R$ we have

$$s(\rho(h_b)u + v) = \rho(h_b)\rho(h_b)^{-1}s\rho(h_b)u + sv \in \rho(h_b)M + M.$$

This shows that J_b is also a left ideal of R . If $J_b = R$, then there are $u, v \in M$ with $1 = \rho(h_b)u + v$. This implies $1 - v = \rho(h_b)u \in R \cap \rho(h_b)R = I_{\rho(h_b)} \subseteq M$ and thus $1 = 1 - v + v \in M$, a contradiction. Thus $(\rho(h_b)M + M) \cap R \neq R$. Since $M \subseteq (\rho(h_b)M + M) \cap R$, we get $M = (\rho(h_b)M + M) \cap R$. But now we have $u\rho(h_a) - \rho(h_a)u \in M$ for all $u \in R$ and thus $\rho(h_a) + M \in Z(R/M)$. But this implies $\rho(h_a) \in Z(J)$, a contradiction. We conclude $\rho(h_b) \in R$. \square

Corollary 4.10 *If $R = J$ is a skewfield, then R is commutative.*

Proof. If $J = R$ is a non-commutative skewfield, then J is not commutative and so $R = S$ by 4.9. But if $b \in A \setminus A_0$, there is a $a \in A_0$ with $\rho(h_a) = -\rho(h_b)$ and so $\rho(h_{ab}) = \rho(h_a) + \rho(h_b) = 0$, but $ab \neq 1$, a contradiction. \square

Proposition 4.11 (a) If $\text{char} R \neq 2$, then $C_A([V, A]) = A_0 = C_A(V/C_V(A))$.

(b) If $\text{char} R = 2$ and R is not a commutative field, then $A_0 = C_A([V, A]) = C_A(V/C_V(A))$.

Proof. Set $A_1 := C_A([V, A])$ and $A_2 := C_A(V/C_V(A))$ and define $B_1, B_2 \leq B$ the same way. Then by 4.6 A_1 and A_2 are both root subgroups of A which contain A_0 and which act quadratically on V . Thus A_1 and A_2 are special. Since A_0 is a H -invariant subgroup of A_0 , Theorem 1.2 in [14] implies $A_1 = A_0 = A_2$ if $\text{char} V \neq 2$.

Suppose $\text{char} V = 2$ and let $a \in A_1$. Then $f(\bar{b}, \bar{a}) = 0$ for all $b \in A$. If a is not in A_2 , then there is an element $b \in A$ with $f(\bar{a}, \bar{b}) \neq 0$. Thus $0 \neq \rho(h_{[a,b]}) = f(\bar{a}, \bar{b})$. Now for $c, d \in A_0$ and $h = h_{[a,b]}^{-1} h_c h_d$, we get

$$\rho(h_c)\rho(h_d) = f(\bar{a}, \bar{b})\rho(h) = f(\bar{a}, \bar{b}^h) = \rho(h_{[a,b^h]}) \in J.$$

Thus J is multiplicatively closed and so $R = J$. Since every element in $J^\#$ is a unit, J is a skewfield. We can apply 4.10 and conclude that $R = J$ is a commutative field if $A_1 \neq A_0$.

For $a \in A_2$ and $b \in A$ we have $f(\bar{b}, \bar{a}) = \rho(h_{[b,a]})$ and thus can use the same argument. \square

We will now define a R -module structure on \bar{A} . For $a \in A$ and $h_1, \dots, h_n \in H_0$ set $\bar{a}^{\sum_i h_i} = \sum_i \bar{a}^{h_i}$.

Proposition 4.12 The map $\cdot : \bar{A} \times R \rightarrow \bar{A}$ defined by $\bar{a} \cdot (\sum_i \rho(h_i)) = \bar{a}^{\sum_i h_i}$ for $h_i \in H_0$ is well-defined and defines a R -module-structure on \bar{A} .

Proof. We only have to show that if $h_1, \dots, h_n \in H_0$ with $\sum_{i=1}^n \rho(h_i) = 0$, then also $\bar{a}^{\sum_{i=1}^n h_i} = \bar{0}$. Suppose that $h_0, \dots, h_n \in H_0$ are chosen that way. Then for all $a, b \in A$ we get

$$0 = f(\bar{a}, \bar{b}) \sum_{i=1}^n \rho(h_i) = f(\bar{a}, \sum_{i=1}^n \bar{b}^{h_i}) = f(\bar{a}, \bar{b}^{\sum_{i=1}^n h_i}).$$

Thus $b^{h_1} \dots b^{h_n} \in C_A([V, A])$. If $A_0 = C_A([V, A])$, then $\bar{b}^{\sum_{i=1}^n h_i} = \bar{0}$. If $A_0 \neq C_A([V, A])$, then R is a field of characteristic 2. Thus H_0 is abelian and $\rho(h^{-\mu}) = \rho(h)$ for all $h \in H_0$ by 4.7. Thus

$$0 = \sum_{i=1}^n \rho(h_i) f(\bar{b}, \bar{a}) = \sum_{i=1}^n \rho(h_i)^{-\mu} f(\bar{b}, \bar{a}) = \sum_{i=1}^n f(\bar{b}^{h_i}, \bar{a}) = f(\bar{b}^{\sum_{i=1}^n h_i}, \bar{a}).$$

Hence we also get $b^{h_1} \dots b^{h_n} \in C_A(V/C_V(A))$ and so the claim follows. \square

Corollary 4.13 *If $\text{char} R \neq 2$, then G is quasi-simple and thus generated by the conjugates of A_0 .*

Proof. If $\text{char} R \neq 2$, then $[\overline{A}, H] = \overline{A}$. Moreover, A' is a H -invariant subgroup of A_0 and thus either $A_0 = A'$ or $A' = 1$. This shows $A \leq G'$ and thus G is perfect. Therefore G is quasi-simple by I(1.10) of [16]. The conjugates of A_0 generate a normal subgroup of G and so the last claim follows. \square

Lemma 4.14 *If A is abelian, then $R/\mathfrak{B}(R)$ is a commutative field of characteristic 2.*

Proof. By 3.10 R must have characteristic 2. Since A is abelian, we have $[a, b] = 1$ for all $a, b \in A$ and thus $f(a, b) = f(b, a)$ by 4.3 (d). We set $I := \{r \in R; f(a, b)r = 0 \text{ for all } a, b \in A\}$. Then I is a right ideal of R . If $r \in I, s \in R$ and $a, b \in A$, then $f(a, b)sr = f(a, b \cdot s)r = 0$ and thus I is an ideal of R . Of course $I \neq R$, otherwise $f(a, b) = 0$ for all $a, b \in A$ and thus G would act quadratically on V . Let $a, b \in A$ and $r, s \in R$. Then

$$\begin{aligned} f(a, b)rs &= f(a, b \cdot r)s = f(b \cdot r, a)s = f(b \cdot r, a \cdot s) = f(a \cdot s, b \cdot r) = f(a \cdot s, b)r = \\ &= f(b, a \cdot s)r = f(b, a)sr = f(a, b)sr. \end{aligned}$$

Thus $rs - sr \in I$. Hence R/I is commutative. Since R/I is an envelope for J , J is commutative. Thus the universal semi-prime envelope of J is a commutative field by 2.6. Since $R/\mathfrak{B}(R)$ is a semi-prime envelope of J , the claim follows. \square

For $n \in \mathbb{Z}$ set $h_n = h_{e^n}$. Note that $\rho(h_n) = n\rho(h_1) = n$ and that $a^{h_n} = a^{n^2}$ for all $a \in A_0$.

Lemma 4.15 *For all $a \in A$ and all $n \in \mathbb{Z}$ such that $n - 1$ and n are relatively prime to the characteristic of A , there is a $b \in A$ with $\overline{a} = \overline{b}$ and $b^n = b^{h_n}$.*

Proof. We have $\overline{a}^{h_n} = \overline{a} \cdot \rho(h_n) = \overline{a}^n = \overline{a^n}$, so $x = a^{h_n}a^{-n} \in A_0$. Since the characteristic of A doesn't divide $n(n-1)$, there is a $y \in A_0$ with $y^{n(n-1)} = x^{-1}$. Set $b = ay$. Then $b^{h_n} = a^{h_n}y^{h_n} = a^nxy^{n^2} = a^ny^n = (ay)^n = b^n$. \square

Lemma 4.16 *If the characteristic of A is not 2, then for all $a \in A$ there is $b \in A$ with $\overline{a} = \overline{b}$ and $f(\overline{a}, \overline{a}) = 2\rho(h_b)$. Especially $f(\overline{a}, \overline{a})$ is a unit in R for $a \notin A_0$.*

Proof. Choose $b \in A$ with $\overline{a} = \overline{b}$ and $b^2 = b^{h_2}$. Then $f(\overline{a}, \overline{a}) = \rho(h_{b^2}) - \rho(h_b) - \rho(h_b) = h_{b^{h_2}} - h_b - h_b = \rho(h_2^{-\mu}h_b h_2) - 2\rho(h_b) = \rho(h_2^{-\mu})\rho(h_b)\rho(h_2) - 2\rho(h_b) = \rho(h_2)\rho(h_b)\rho(h_2) - 2\rho(h_b)4\rho(h_b) - 2\rho(h_b) = 2\rho(h_b)$. If $a \notin A_0$, then $b \neq 1$ and so $\rho(h_b)$ is invertible. \square

We will now show that the anti-automorphism $h \mapsto h^{-\mu}$ extends uniquely to

an anti-automorphism $*$ of R . Note that this is clear if H_0 is abelian and that $*$ is just the identity or R in this case. This holds by 4.7 (b) and since H_0 is generated by the elements h_a with $a \in A_0^\#$.

Proposition 4.17 *There is a unique involutory anti-automorphism $*$ of R with $\rho(h_b)^* = \rho(h_b^{-\mu})$ for all $b \in A_0$.*

Proof. The map $h \mapsto h^{-\mu}$ is an anti-automorphism of H_0 . Since R is generated by $\rho(H_0)$, there is at most one possibility to extend this map to an anti-automorphism of R . We have to show that if $h_1, \dots, h_n \in H_0$ with $\sum_{i=1}^n \rho(h_i) = 0$, then also $\sum_{i=1}^n \rho(h_i^{-\mu}) = 0$. In this case, the map $*$ with $(\sum_{i=1}^n \rho(h_i))^* = \sum_{i=1}^n \rho(h_i^{-\mu})$ for $h_1, \dots, h_n \in H_0$ is a well-defined anti-automorphism of R . Suppose that $h_1, \dots, h_n \in H_0$ with $\sum_{i=1}^n \rho(h_i) = 0$. By the remark above and by 4.14 we may assume that A is not abelian. Thus by 4.3 (d) and by 4.16 there is an element $a \in A$ such that $f(a, a)$ is a unit in R . Therefore we get

$$0 = f(\bar{0}, \bar{a}) = f(\bar{a} \cdot \sum_{i=1}^n \rho(h_i), \bar{a}) = \sum_{i=1}^n f(\bar{a} \cdot \rho(h_i), \bar{a}) = \sum_{i=1}^n \rho(h_i^{-\mu}) f(\bar{a}, \bar{a}).$$

This implies $\sum_{i=1}^n \rho(h_i^{-\mu}) = 0$, as desired. \square

Proposition 4.18 (a) *The map $f : \bar{A} \times \bar{A} \rightarrow S$ is $*$ -sesquilinear.*

(b) *If J is not a field of characteristic 2, then f is non-degenerate.*

(c) *If J is commutative, then the map $(\cdot, \cdot) : \bar{A} \times \bar{A} \rightarrow R : (\bar{a}, \bar{b}) \mapsto f(a, b) - f(b, a) = \rho(h_{[a, b]})$ is an alternating R -bilinear map.*

Proof.

(a) This follows by 4.3 (a) and (b), 4.5, 4.12 and 4.17.

(b) This follows by 4.3 (c) and 4.11.

(c) If J is commutative, then $*$ is the identity, so f is R -bilinear. By 4.3 (d), $(\bar{a}, \bar{b}) = f(a, b) - f(b, a)$, so (\cdot, \cdot) is also R -bilinear. It is clear that (\cdot, \cdot) is alternating. \square

Lemma 4.19 *If $\text{char} R = 2$ and A is not abelian, then J is ample in R .*

Proof. Since A is not abelian, there is an element $a \in A$ with $a^2 = e$. Thus $f(\bar{a}, \bar{a}) = \rho(h_e) = 1$. If $r \in R$ and $b \in A$ with $\bar{b} = \bar{a} \cdot r$ we get $r^*r = f(\bar{a} \cdot r, \bar{a} \cdot r) = f(\bar{b}, \bar{b}) = \rho(h_{b^2}) \in J$. This also implies

$$r + r^* = (r + 1)^*(r + 1) + r^*r + 1 \in J.$$

Now set $N_R(J) := \{r \in R; r^*Jr \subseteq J\}$. Then $J \subseteq N_R(J)$ since $\rho(h_b)^*\rho(h_a)\rho(h_b) = \rho(h_{ah_b}) \in J$ for all $a, b \in A_0$. If $r, s \in N_R(J)$, then $(rs)^*J(rs) = s^*r^*Jrs \subseteq s^*Js \subseteq J$ and so also $rs \in J$. For $x \in J$, we get

$$(r + s)^*x(r + s) = r^*xr + s^*xs + r^*xs + s^*xr = r^*xr + s^*xs + r^*xs + (r^*xs)^* \in J,$$

thus $r + s \in N_R(J)$. Hence $N_R(J)$ is a ring containing J ; since J generates R as a ring, we get $R = N_R(J)$. \square

Theorem 4.20 (a) *If $\text{char} R \neq 2$, then R is a skewfield.*

(b) *If $\text{char} R = 2$, then one of the following holds:*

(i) *$R/\mathfrak{B}(R)$ is a skewfield.*

(ii) *$R/\mathfrak{B}(R) \cong K \times K^o$ for a skewfield K and $*$ induces the exchange involution on R .*

Proof.

(a) If $r \in R$ and $a \in A \setminus A_0$ with $\bar{a} \cdot r = \bar{0}$, then $0 = f(\bar{a}, \bar{a} \cdot r) = f(\bar{a}, \bar{a})r$. But $f(\bar{a}, \bar{a})$ is a unit in R since $a \notin A_0$, thus $r = 0$. So if $r \neq 0$, then $\bar{a} \cdot r \neq 0$ and thus $f(\bar{a} \cdot r, \bar{a} \cdot r)$ is again a unit. We get $r^*f(\bar{a}, \bar{a})r = f(\bar{a} \cdot r, \bar{a} \cdot r)$ and $rf(\bar{a}, \bar{a})r^* = f(\bar{a} \cdot r^*, \bar{a} \cdot r^*)$. Hence r is invertible.

(b) If A is abelian, then the claim follows by 4.14. If A is not abelian, then J is ample in R . By Theorem 2.1.8 in [7], $R/\mathfrak{B}(R)$ is either a skewfield, or $R/\mathfrak{B}(R)$ is commutative and $*$ induces the identity on $R/\mathfrak{B}(R)$, or $R/\mathfrak{B}(R)$ is the direct product of a skewfield and its opposite and $*$ induces the exchange involution on $R/\mathfrak{B}(R)$, or $R/\mathfrak{B}(R) \cong \text{Mat}_2(F)$ for a commutative field F and $*$ induces the standard involution on $R/\mathfrak{B}(R)$ (which is given by

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}^* = \begin{pmatrix} w & y \\ z & x \end{pmatrix}$$

for $x, y, z, w \in F$). If $R/\mathfrak{B}(R)$ is commutative, J must be commutative as well. Since $R/\mathfrak{B}(R)$ is the semi-prime envelope of J , $R/\mathfrak{B}(R)$ must be a field. Suppose the last case holds. Let \bar{J} be the image of J in $\bar{R} := R/\mathfrak{B}(R)$. Since J contains all traces, $Z(\bar{R}) \subseteq \bar{J}$. Since R is generated by J , \bar{J} cannot be $Z(\bar{R})$. Therefore there are $x, y \in F$ with

$$0 \neq \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \in \bar{J}.$$

Since every element in $J^\#$ is invertible, neither x nor y can be 0. But since J is ample in R , we get

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} \in \overline{J},$$

a contradiction, since every element in $J^\#$ is invertible. Thus the last case cannot hold. \square

Theorem 4.21 *If J is not commutative, then $R = S$ and $R/\mathfrak{B}(R)$ is a skewfield. If $\text{char} R \neq 2$, then R is a skewfield.*

Proof. By 4.20 $R/\mathfrak{B}(R)$ and therefore R has at most 2 maximal ideals. So we can apply 4.9 and conclude $R = S$. Because of 4.20 we only have to show that if $\text{char} R = 2$, then $R/\mathfrak{B}(R) \cong K \times K^o$ for a skewfield K is not possible. Suppose that $R/\mathfrak{B}(R) = K \times K^o$. We denote the anti-isomorphism induced by $*$ on $K \times K^o$ also by $*$. There is an anti-automorphism $\phi : K \rightarrow K^o$ such that $(x, y)^* = (y^{\phi^{-1}}, x^\phi)$ for $x \in K, y \in K^o$. Thus the image of J is the set $\{(x, x^\phi); x \in K\}$. If $b \in A \setminus A_0$, then $\overline{\rho(b)}$ is mapped on (x, y) with $x \in K, y \in K^o$. But then there is a $a \in A_0$ such that $\rho(h_a)$ is mapped on (x, x^ϕ) and so $\rho(h_{ba})$ is mapped on $(0, x^\phi + y)$, a contradiction, since $\rho(h_{ba})$ is invertible. \square

In the most cases $\mathfrak{B}(R)$ is actually 0 and so R is a skewfield.

Proposition 4.22 *If J is not commutative and $\mathfrak{B}(R) \neq 0$, then either $R/\mathfrak{B}(R)$ is a biquaternion algebra, $*$ induces a symplectic involution on $R/\mathfrak{B}(R)$ and $J \cong K_* = \{a + a^*; a \in K\}$, or $R/\mathfrak{B}(R)$ is a quaternion algebra.*

Proof. Set $K := R/\mathfrak{B}(R)$ and let K_0 be the image of J in K . Then there is a Jordan isomorphism $\phi : K_0 \rightarrow J$. If $Z_{48}(K_0) \neq 0$, then by the Z -algebra Theorem ([10]) ϕ can be extended to an associative homomorphism $\tilde{\phi} : K \rightarrow R$. Since $J \subseteq \text{im} \phi$ and J generates R , we have $R = \text{im} \phi \cong K$. Now 2.6.5. in [9] tells us that $Z_{48}(K_0) = 0$ implies that either K is a biquaternion algebra, $*$ a symplectic involution and $K_0 = K_*$, or K is a quaternion algebra. \square

5 Irreducible submodules of V

In this chapter we will show that if R is a skewfield, then one can reduce to the case that V is irreducible as a G -module. We will not need any finiteness assumption. We define

$$\Phi : C_V(A) \times A \rightarrow C_V(G_0) : (v, a) \mapsto [v\mu, a] - v h_a.$$

This is well-defined by 4.2. This important map reveals the connection between \overline{A} and $C_V(G_0)$.

Lemma 5.1 (a) Φ is a biadditive map from $C_V(A) \times A$ to $C_V(G_0)$.

(b) $\Phi(vh, a) = \Phi(v, a^{h^{-\mu}})$ for all $v \in C_V(A)$, $a \in A$ and $h \in H_0$.

(c) $C_A(V/C_V(A))$ is the right kernel of Φ .

Proof.

(a) It is clear that $\Phi(v + w, a) = \Phi(v, a) + \Phi(w, a)$ holds for all $v, w \in C_V(A)$ and all $a, b \in A$. If $v \in C_V(A)$ and $a, b \in A$, then

$$\begin{aligned}\Phi(v, ab) &= [v\mu, ab] - vh_{ab} = -v\mu + v\mu ab - vh_a - vh_b - vf(a, b) = \\ &= -v\mu + (v\mu + [v\mu, a])b - vh_a - vh_b - vf(a, b) = -v\mu + v\mu b + [v\mu, a]b - vh_a - vh_b - [v\mu, a, b] = \\ &= [v\mu, a] - vh_a + [v\mu, b] - vh_b + [v\mu, a, b] - [v\mu, a, b] = \\ &= [v\mu, a] - vh_a + [v\mu, b] - vh_b = \Phi(v, a) + \Phi(v, b).\end{aligned}$$

(b) For $v \in C_V(A)$, $h \in H_0$ and $a \in A$ we have $\Phi(v, a) \in C_V(h^{-\mu})$. Thus we get

$$\begin{aligned}[vh\mu, a] - vhh_a &= ([v\mu h^\mu, a] - vhh_a)h^{-\mu} = -v\mu h^\mu h^{-\mu} + v\mu h^\mu ah^{-\mu} - vh^\mu h_a h^{-\mu} = \\ &= -v\mu + v\mu a^{h^{-\mu}} - vh_{ah^{-\mu}} = [v\mu, a^{h^{-\mu}}] - vh_{ah^{-\mu}} = \Phi(v, a^{h^{-\mu}}).\end{aligned}$$

(c) Suppose $a \in A$ with $[v\mu, a] - vh_a = 0$ for all $v \in C_V(A)$. Then we have

$$[V, a] = [[V, A] \oplus C_V(B), a] \leq C_V(A) + [C_V(A)\mu, a] \leq C_V(A)$$

and thus $a \in C_A(V/C_V(A))$. If $a \in C_A(V/C_V(A))$, then

$$[v\mu, a] - vh_a \in C_V(A) \cap C_V(G_0) = C_V(A) \cap [V, B] = 0.$$

Thus the claim follows. □

The right kernel of Φ contains A_0 by (c). Therefore we may regard Φ as a map from $C_V(A) \times \overline{A}$ to $C_V(G_0)$.

Let W be a H -submodule of $C_V(A)$. We set $X(W) := W + W\mu + \Phi(W, A)$. Then we have:

Lemma 5.2 (a) $X(W)$ is a G -submodule of V .

(b) $X(W) \cap C_V(A) = W$, $X(W) \cap C_V(B) = W\mu$.

(c) $[X(W), A] = W + \Phi(W, A)$ and $X(W) \cap C_V(G_0) = \Phi(W, A)$.

(d) $X(W)$ is the direct sum of W , $W\mu$ and $\Phi(W, A)$.

- (e) W is a irreducible H -module iff $X(W)$ is a irreducible G -module.
- (f) V is a completely reducible G -module iff $C_V(A)$ is a completely reducible H -module.

Proof.

- (a) We only have to show that $X(W)$ is normalized by A and by μ since $G = \langle A, \mu \rangle$. If $w \in W$, then $w\mu \in W\mu \subseteq X(W)$ and $w\mu^2 = -w \in W \subseteq X(W)$. Moreover, $\Phi(W, A) \subseteq C_V(G_0) \subseteq C_V(\mu)$, so $X(W)$ is μ -invariant. Suppose $a, b \in A$ and $w \in W$. Then $wa = w \in W$,

$$w\mu a = w\mu + [w\mu, a] = w\mu + [w\mu, a] - wh_a + wh_a =$$

$$w\mu + \Phi(w, a) + wh_a \in W\mu + \Phi(W, A) + W = X(W)$$

and

$$\begin{aligned} \Phi(w, b)a &= ([w\mu, b] - wh_b)a = [w\mu, b]a - wh_b = [w\mu, b] + [w\mu, b, a] - wh_b \\ &= \Phi(w, b) - wf(b, a) \in \Phi(W, A) + W \subseteq X(W). \end{aligned}$$

Thus the claim follows.

- (b) This is clear since $V = C_V(A) \oplus (C_V(G_0)) \oplus C_V(B)$ and $W \subseteq C_V(A)$, $W\mu \subseteq C_V(B)$ and $\Phi(W, A) \subseteq C_V(G_0)$.
- (c) We have $W = [W\mu, A_0] \leq [X(W), A]$ and so $\Phi(w, a) = [w\mu, a] - vha \in [X(W), A] + W = [X(W), A]$, thus $W + \Phi(W, A) \leq [X(W), A]$. Since $[W\mu, A] \leq \Phi(W, A) + W$, $[\Phi(W, A), A] \leq W$ and $[W, A] = 0$, we get equality. Surely $\Phi(W, A) \leq C_V(G_0)$. Since $(W + W\mu) \cap C_V(G_0) = 0$, equality must hold.
- (d) This follows from (b) and (c).
- (e) Suppose W is a irreducible H -module and let $0 \neq Y$ be a G -submodule of $X(W)$. Then $[Y, A] \neq 0$. If $[Y, A, A] = 0$, then $[Y, A] \subseteq C_V(A) = C_V(A)$ and so $C_V(A) \cap Y \neq 0$. If $[Y, A, A] \neq 0$, then of course we also have $Y \cap C_V(A) \neq 0$, so this holds in any case. Since $0 \neq Y \cap C_V(A) \subseteq X(W) \cap C_V(A) = W$ and W is a irreducible H -module, we get $Y \cap C_V(A) = W$. Then also $W\mu \cap Y$ and $\phi(w, a) = [w\mu, a] - wh_a \in Y + W = Y$ for all $w \in W, a \in A$. Thus $Y = X(W)$.
If $0 \neq W_0 \neq W$ is a H -submodule of W , then $X(W_0)$ is a G -submodule of $X(W)$ with $X(W_0) \cap C_V(A) = W_0 \neq W = X(W) \cap C_V(A)$ and thus $X(W_0) \neq X(W)$.
- (f) Suppose $C_V(A) = \sum_{i \in I} W_i$ is a direct decomposition of $C_V(A)$ as a sum of irreducible H -modules. We claim that $V = \sum_{i \in I} X(W_i)$ is a direct decomposition of V as a sum of irreducible G -modules. If $X := \sum_{i \in I} X(W_i)$, then $C_V(A), C_V(B) \subseteq X$ and so $A_0 \leq C_G(V/X)$. This

implies $G = AC_G(V/X)$ and $V = X + (C_V(G_0))$. But then we have $[V, A] \subseteq [X, A] + C_V(A) \subseteq X$ and so $[V/X, A] = 0$. This implies $X = V$. Suppose that the sum is not direct. Then there is an element $i \in I$ and a finite subset I_0 of I with $i \notin I_0$ and $X(W_i) \cap (\sum_{j \in I_0} X(W_j)) \neq 0$. Since $X(W_i)$ is a irreducible G -module, this implies $X(W_i) \subseteq \sum_{j \in I_0} X(W_j)$. But then we also have $W_i = X(W_i) \cap C_V(A) \subseteq C_V(A) \cap (\sum_{j \in I_0} X(W_j)) = \sum_{j \in I_0} X(W_j)$, as one can easily see. But this is a contradiction since the decomposition of $C_V(A)$ is direct.

Suppose $V = \sum_{i \in I} V_i$ such that V_i is irreducible for all $i \in I$ and that this sum is direct. Then, as seen in (e), $V_i \cap C_V(A) \neq 0$. Therefore $0 \neq X(V_i \cap C_V(A))$ and so $V_i = X(V_i \cap C_V(A))$. Since V_i is irreducible, it follows by (e) that $V_i \cap C_V(A)$ is a irreducible H -module. Set $W = \sum_{i \in I} (V_i \cap C_V(A))$. Then $V_i = X(C_V(A) \cap V_i) \subseteq X(W)$ for all $i \in I$ and so $X(W) = V$. Thus $W = X(W) \cap C_V(A) = V \cap C_V(A) = C_V(A)$. Since $\sum_{i \in I} V_i$ is direct, also $\sum_{i \in I} (C_V(A) \cap V_i)$ is direct.

□

Corollary 5.3 *If S is a skewfield or a finite-dimensional central-simple algebra, then V is a completely reducible G -module.*

Proposition 5.4 *Suppose that $R = S$ and that A is not abelian. If $v \in C_V(A)$ with $\Phi(v, a) = 0$ for all $a \in A$, then $v = 0$.*

Proof. Let $W = vR$. Then W is H -invariant since R is generated by $\rho(H)$. If $r \in R$, then $r = \sum_{i=1}^n h_i$ with $h_i \in H_0$. Thus for all $a \in A$ we get

$$\Phi(vr, a) = \Phi\left(\sum_{i=1}^n v h_i, a\right) = \sum_{i=1}^n \Phi(v h_i, a) = \sum_{i=1}^n \Phi(v, a^{h_i^{-\mu}}) = 0.$$

Thus $W \oplus W\mu = X(W)$ is a quadratic G -module. Thus $A/C_A(X(W))$ must be abelian. We conclude $W\mu \leq C_V(a)$ for all $a \in A_0$. Since $1 \neq A' \leq A_0$, we get $W = 0$ by 3.11.

□

Lemma 5.5 *If $R = S$ and $W \subseteq C_V(A)$ is H -invariant, then $[X(W), G] = X(W)$ and $C_{X(W)}(G) = 0$.*

Proof. $C_{X(W)}(G) = 0$ is clear since $C_V(G) = 0$. $X(W) = [X(W), G]$ follows with 5.2(c).

□

Suppose that $\text{char } R = 2$, J is not commutative. Then $R = S$ and $R/\mathfrak{B}(R)$ is a skewfield. Moreover, A is not abelian, so there is $c \in A$ with $f(c, c) = 1$. Let $W \leq C_V(A)$ be a finitely generated R -module. Define $A_1 := \{a \in A; f(\bar{a}, \bar{b}) \in \mathfrak{B}(R) \text{ for all } b \in A\}$, $H_1 := \{\mu\mu_a; a \in A_1\}$ and $\bar{X}(W) := X(W)/(X(W)\mathfrak{B}(R)) + \Phi(W, A_1)$. Then we have:

Proposition 5.6 *If $W \neq 0$, then $0 \neq \overline{X}(W)$ is a cubic module for G with $A_1 = C_A([\overline{X}(W), A]) \cap C_A(\overline{X}(W)/C_{\overline{X}(W)}(A))$, $\overline{X}(W) = [\overline{X}(W), G]$ and $C_{\overline{X}(W)}(G) = 0$. If R' is the subring of $\text{End}(\overline{X}(W))$ generated by H_0 , then $R' = R/\mathfrak{B}(R)$.*

Proof. First note that $[\Phi(W, A_1), A] \leq W\mathfrak{B}(R)$ and $\Phi(W, A_1) \leq C_V(\mu)$; this implies that $X(W\mathfrak{B}(R)) + \Phi(W, A_1)$ is a G -submodule of $X(W)$. If $W \neq 0$, then $W \neq W\mathfrak{B}(R)$ by the Nakayama Lemma (note that $\mathfrak{B}(R) \subseteq J(R)$). Thus we also get $X(W) \neq X(W\mathfrak{B}(R)) + \Phi(W, A_1)$. Now $X(W) = [X(W), G]$ and thus $[\overline{X}(W), G] = \overline{X}(W)$. Thus $[\overline{X}(W), G, G, G] \neq 0$ and $[\overline{X}(W), A, A, A] = 0$, so $\overline{X}(W)$ is a cubic module for G .

Suppose that $z \in C_{\overline{X}(W)}(G)$. Since $K = R/\mathfrak{B}(R)$ is a skewfield, $W/W\mathfrak{B}(R)$ is a finite-dimensional vectorspace over K . Let $\{\overline{w}_1, \dots, \overline{w}_n\}$ be a K -basis of \overline{W} and let w_1, \dots, w_n be their preimages in W . Then $W = w_1R + \dots + w_nR + W\mathfrak{B}(R)$ and so $W = w_1R + \dots + w_nR$. Thus there are $x, y \in W, a_1, \dots, a_n \in A$ with $z = x + \Phi(w_1, a_1) + \dots + \Phi(w_n, a_n) + y\mu + X(W\mathfrak{B}(R)) + \Phi(W, A_1)$. We get $0 = [z, e] = [y, e] + X(W\mathfrak{B}(R)) + \Phi(W, A_1)$ and thus $y = [y\mu, e] \in W\mathfrak{B}(R)$. If we apply μ , we get $x \in W\mathfrak{B}(R)$. For all $a \in A$ we have

$$0 = [z, a] = w_1f(\overline{a}_1, \overline{a}) + \dots + w_nf(\overline{a}_n, \overline{a}) + X(W\mathfrak{B}(R)) + \Phi(W, A_1)$$

and therefore

$$w_1f(\overline{a}_1, \overline{a}) + \dots + w_nf(\overline{a}_n, \overline{a}) \in W\mathfrak{B}(R).$$

Since $\overline{w}_1, \dots, \overline{w}_n$ are K -linearly independent, this implies $f(\overline{a}_1, \overline{a}), \dots, f(\overline{a}_n, \overline{a}) \in \mathfrak{B}(R)$. Thus $a_1, \dots, a_n \in A_1$ and so $z = 0$.

By 5.2 (b) one sees that $C_A(\overline{X}(W))$ is just the image of W in $\overline{X}(W)$. Thus $C_A(\overline{X}(W)/C_A(\overline{X}(W))) = A_1$. Since J is not commutative, we also have $A_1 = C_A([\overline{X}(W), A])$ by 4.11.

Since $H_1 \leq H$, the ring R' is contained in the image of $R = S$ in $\text{End}(\overline{X}(W))$. Now $\mathfrak{B}(R)$ annihilates $\overline{X}(W)$ by construction. Thus we get $R' = R/\mathfrak{B}(R)$ which is a skewfield. \square

This proposition shows that we can assume that R is a skewfield if J is not commutative.

6 A pseudo-quadratic form on \overline{A}

In this section we will assume that J is not commutative and that $\mathfrak{B}(R) = 0$. Thus R is a skewfield with involution $*$. We have $J \subseteq H(R, *)$. If $\text{char} R = 2$, then J is ample in R .

Lemma 6.1 (a) *If $a \in A$, then $\rho(h_a) \in J$ iff $a \in A_0$.*

(b) *If $\text{char} R \neq 2$, then $\rho(h_a) \in H(R, *)$ iff $a \in A_0$.*

Proof.

- (a) Let $a \in A$ with $\rho(h_a) \in J$. Then there is $b \in A_0$ with $\rho(h_b) = -\rho(h_a)$ and thus $\rho(h_{ab}) = \rho(h_a) + \rho(h_b) = 0$. Thus $ab = 1$ and $a = b^{-1} \in A_0$.
- (b) Suppose that $a \in A$ with $-\rho(h_{a^{-1}}) = (\rho(h_a))^* = \rho(h_a)$. Then for $b \in A_0$ we have $\rho(h_{ab})^* = (\rho(h_a) + \rho(h_b))^* = \rho(h_a) + \rho(h_b) = \rho(h_{ab})$. By 4.15 we may thus assume that $a^{h^{-1}} = a^{-1}$. So we get

$$\rho(h_a) = \rho(h_a)^* = -\rho(h_{a^{-1}}) = -\rho(h_{a^{h^{-1}}}) = -\rho(h_{-1}h_a h_{-1}) = -\rho(h_a)$$

and so $\rho(h_a) = 0$. This forces $a = 1$.

□

Lemma 6.2 *We have $\rho(h^{-\mu}) = \rho(h)^*$ for all $h \in H$.*

Proof. We consider the action of G_0H on $X := C_V(A) \oplus C_V(B)$. We regard R as a subring of $E := \text{End}(C_V(A))$. The map μ induces an automorphism between $C_V(A)$ and $C_V(B)$. Thus we can regard X as a free E -module of rank 2. Therefore we get a homomorphism ξ from G_0H in the group of all invertible 2×2 -matrices over R , such that the image of $a \in A_0$ is

$$\begin{pmatrix} 1 & 0 \\ \rho(h_a) & 1 \end{pmatrix},$$

while μ is mapped to

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and h_a is mapped to

$$\begin{pmatrix} \rho(h_a) & 0 \\ 0 & \rho(h_a)^{-1} \end{pmatrix} = \begin{pmatrix} \rho(h_a) & 0 \\ 0 & \rho(h_a)^{-*} \end{pmatrix}.$$

For $b \in A$ there is an element $y \in R$ such that the image of h_b is

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$$

with $x = \rho(h_b)$. We get

$$\xi(h_b^{-1}ah_b) = \begin{pmatrix} 1 & 0 \\ y^{-1}\rho(h_a)x & 1 \end{pmatrix}.$$

Thus we have

$$y^{-1}\rho(h_a)x = (y^{-1}\rho(h_a)x)^* = x^*\rho(h_a)y^{-*}$$

and hence

$$\rho(h_a) = yx^*\rho(h_a)y^{-*}x^{-1} = (yx^*)\rho(h_a)(yx^*)^{-*}$$

for all $a \in A_0$. If we take $a = e$, we get $(yx^*)^{-1} = (yx^*)^{-*}$ and thus $(yx^*)^* = yx^*$. Therefore we have $(yx^*)\rho(h_a)(yx^*)^{-1} = \rho(h_a)$ for all $a \in A_0$. Since R is generated by $\rho(H_0)$, we conclude $yx^* \in k := H(Z(R), *)$. Thus for all $b \in A^\#$ there is a $\omega_b \in k$ with

$$\xi(h_b) = \begin{pmatrix} \rho(h_b) & 0 \\ 0 & \rho(h_b)^{-*}\omega_b \end{pmatrix}.$$

Of course, $\omega_a = 1$ for all $a \in A_0$. We have $h_b^{-\mu} = (\mu^{-1}\mu\mu_b\mu)^{-1} = \mu^{-1}\mu_b^{-1} = \mu^{-1}\mu_{b^{-1}} = \mu^2 h_{b^{-1}}$ and thus

$$\begin{aligned} & \begin{pmatrix} -\rho(h_{b^{-1}}) & 0 \\ 0 & -\rho(h_{b^{-1}})^{-*}\omega_{b^{-1}} \end{pmatrix} = \xi(\mu^2)\xi(h_{b^{-1}}) = \xi(h_b^{-\mu}) \\ & = \xi(\mu)^{-1}\xi(h_b)^{-1}\xi(\mu) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \rho(h_b)^{-1} & 0 \\ 0 & \rho(h_b)^*\omega_b^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ & = \begin{pmatrix} \rho(h_b)^*\omega_b^{-1} & 0 \\ 0 & -\rho(h_b)^{-1} \end{pmatrix}. \end{aligned}$$

Hence $\rho(h_b)^* = -\omega_b\rho(h_{b^{-1}}) = \omega_b\rho(h_b^{-\mu})$ for all $b \in A$. For $a \in A_0$ we get

$$\begin{aligned} \rho(h_a) - \omega_b\rho(h_{b^{-1}}) &= \rho(h_a)^* + \rho(h_b)^* = \rho(h_{ba})^* = \\ &= -\omega_{ab}\rho(h_{a^{-1}b^{-1}}) = -\omega_{ab}(\rho(h_{a^{-1}}) + \rho(h_{b^{-1}})) \\ &= \omega_{ab}\rho(h_a) - \omega_{ab}\rho(h_{b^{-1}}). \end{aligned}$$

We get

$$(1 - \omega_{ab})\rho(h_a) = (\omega_b - \omega_{ab})\rho(h_{b^{-1}}).$$

If $1 - \omega_{ab} \neq 0$, then also $\omega_b - \omega_{ab} \neq 0$ and so

$$\rho(h_{b^{-1}}) = (\omega_b - \omega_{ab})^{-1}(1 - \omega_{ab})\rho(h_a).$$

If $\text{char} R \neq 2$, this forces $\rho(h_{b^{-1}})^* = \rho(h_{b^{-1}})$, a contradiction to 6.1. If $\text{char} R = 2$, then J contains all traces by 4.19, thus there is $a \in A_0$ and $r \in R$ with $\rho(h_a) = r + r^*$. Thus

$$\begin{aligned} \rho(h_{b^{-1}}) &= (\omega_b - \omega_{ab})^{-1}(1 - \omega_{ab}(r + r^*)) = \\ &= (\omega_b - \omega_{ab})^{-1}(1 - \omega_{ab})r + ((\omega_b - \omega_{ab})^{-1}(1 - \omega_{ab})r)^* \in J \end{aligned}$$

by 4.19, again a contradiction to 6.1. So $\omega_b = 1$ for all $b \in A^\#$. Thus $\rho(h_b)^* = -\rho(h_{b^{-1}}) = \rho(h_b^{-\mu})$ for all $b \in A$. \square

Lemma 6.3 *f is *-skew-hermitian.*

Proof. For all $a, b \in A$ we have $f(\bar{a}, \bar{b}) = \rho(h_{ab}) - \rho(h_a) - \rho(h_b)$ and so

$$\begin{aligned} f(\bar{a}, \bar{b})^* &= \rho(h_{ab})^* - \rho(h_a)^* - \rho(h_b)^* = -\rho(h_{(ab)^{-1}}) + \rho(h_{a^{-1}}) + \rho(h_{b^{-1}}) = \\ &= -(\rho(h_{b^{-1}a^{-1}}) - \rho(h_{b^{-1}}) - \rho(h_{a^{-1}})) = -f(\bar{b}^{-1}, \bar{a}^{-1}) = f(\bar{b}, \bar{a}^{-1}) = -f(\bar{b}, \bar{a}). \end{aligned}$$

□

Lemma 6.4 *If $\text{char} R \neq 2$, then $J = H(R, *)$.*

Proof. For all $a, b \in A$ we have

$$f(\bar{a}, \bar{b}) + f(\bar{a}, \bar{b})^* = f(\bar{a}, \bar{b}) - f(\bar{b}, \bar{a}) = \rho(h_{[a, b]}) \in J.$$

Since A is not abelian, there are $a, b \in A$ with $[a, b] \neq 1$ and thus $\rho([a, b]) \neq 0$. For all $r \in R$ we get $f(\bar{a}, \bar{b} \cdot f(\bar{a}, \bar{b})^{-1}r) = r$ and hence $r + r^* \in J$. Since $\text{char} R \neq 2$, we have $H(R, *) = \{r + r^*; r \in R\}$ and thus the claim follows. □

Lemma 6.5 *The map $\pi : A/A_0 \rightarrow R/J : b + A_0 \mapsto \rho(h_b)$ is a pseudo-quadratic form with associated bilinear form f .*

Proof. We first note that π is well-defined since

$$\rho(h_{ab}) = \rho(h_a) + \rho(h_b) \equiv \rho(h_b) \text{ mod } J$$

for all $a \in A_0, b \in A$. Since $r + r^* \in J$ for all $r \in R$ in any characteristic, we have $r^* \equiv r^* - (r + r^*) \equiv -r \text{ mod } J$. If $r \in R$, then there is a natural number n and elements $h_1, \dots, h_n \in H_0$ with $r = \sum_{i=1}^n \rho(h_i)$. Thus if $b \in A$, then we get

$$\pi(\bar{b} \cdot r) = \pi(\bar{b} \cdot h_1 + \dots + \bar{b} \cdot h_n) = \rho(h_{b^{h_1} \dots b^{h_n}}) + J = \sum_{i=1}^n \rho(h_{b^{h_i}}) + \sum_{i < j} f(\bar{b}^{h_i}, \bar{b}^{h_j}) + J =$$

$$\begin{aligned} &\sum_{i=1}^n \rho(h_i^{-\mu} h_b h_i) + \sum_{i < j} \rho(h_i^{-\mu}) f(\bar{b}, \bar{b}) \rho(h_j) = \\ &\sum_{i=1}^n \rho(h_i)^* \rho(h_b) \rho(h_i) + \sum_{i < j} \rho(h_i)^* f(b, b) \rho(h_j). \end{aligned}$$

We have

$$\begin{aligned} 0 &= \rho(h_1) = \rho(h_{bb^{-1}}) = \rho(h_b) + \rho(h_{b^{-1}}) + f(\bar{b}, \bar{b}^{-1}) = \\ &= \rho(h_b) + \rho(-h_b^{-\mu}) + f(\bar{b}, -\bar{b}) = \rho(h_b) - \rho(h_b^{-\mu}) - f(\bar{b}, \bar{b}) \end{aligned}$$

and thus

$$f(\bar{b}, \bar{b}) = \rho(h_b) - \rho(h_b^{-\mu}) = \rho(h_b) - \rho(h_b)^*.$$

Thus we get

$$\rho(h_i)^* f(\bar{b}, \bar{b}) \rho(h_j) = \rho(h_i)^* (\rho(h_b) - \rho(h_b)^*) \rho(h_j) =$$

$$\rho(h_i)^* \rho(h_b) \rho(h_j) - (\rho(h_j)^* \rho(h_b) \rho(h_i))^*.$$

Since

$$-(\rho(h_j)^* \rho(h_b) \rho(h_i))^* \equiv \rho(h_j)^* \rho(h_b) \rho(h_i) \mod J,$$

we get

$$\rho(h_i)^* f(\bar{b}, \bar{b}) \rho(h_j) \equiv \rho(h_i)^* \rho(h_b) \rho(h_j) + \rho(h_j)^* \rho(h_b) \rho(h_i) \mod J.$$

Therefore

$$\begin{aligned} \pi(\bar{b} \cdot r) &\equiv \sum_{i=1}^n \rho(h_i)^* \rho(h_b) \rho(h_i)^* + \sum_{i \neq j} \rho(h_i)^* \rho(h_b) \rho(h_j) \equiv \sum_{i,j=1}^n \rho(h_i)^* \rho(h_b) \rho(h_j) \\ &\equiv (\rho(h_1) + \dots + \rho(h_n))^* \rho(h_b) (\rho(h_1) + \dots + \rho(h_n)) \equiv r^* \pi(\bar{b}) r \mod J. \end{aligned}$$

The equation

$$\pi(\bar{b} + \bar{c}) \equiv \pi(\bar{b}) + \pi(\bar{c}) + f(\bar{b}, \bar{c}) \mod J$$

already follows from 4.4. □

7 A pseudo-quadratic form on V

In this section we continue to assume that J is not commutative, so R is a skewfield with involution $*$. We additionally assume that $\dim_R C_V(A) = 1$. This implies that G acts irreducibly on V . We have defined an anisotropic pseudo-quadratic form on the R -vectorspace \bar{A} . We will make V to a vectorspace over R and translate this form to a form of V .

From now on, let $0 \neq v \in C_V(A)$ be fixed.

Lemma 7.1 *The map $\Phi(v, \cdot) : \bar{A} \rightarrow \Phi(V, A)$ is an isomorphism with*

$$\Phi(v, \bar{a} \cdot r) = \Phi(v, \bar{a}) r^*$$

for all $\bar{a} \in \bar{A}$ and all $r \in$.

Proof. If $w \in C_V(A)$, $a \in A$ and $h \in H_0$, then by 5.1

$$\begin{aligned} \Phi(w \rho(h), \bar{a}) &= \Phi(w h, \bar{a}) = \Phi(w, \bar{a}^{h^{-\mu}}) = \Phi(w, \bar{a} \cdot \rho(h^{-\mu})) = \\ &= \Phi(w, \bar{a} \cdot \rho(h)^*). \end{aligned}$$

Now there are $h_1, \dots, h_n \in H_0$ with $w = \sum_{i=1}^n v \rho(h_i)$. Then for all $\bar{a} \in \bar{A}$ we get

$$\Phi(w, \bar{a}) = \Phi(v \sum_{i=1}^n \rho(h_i), \bar{a}) = \sum_{i=1}^n \Phi(v \rho(h_i), \bar{a}) = \sum_{i=1}^n \Phi(v, \bar{a} \cdot \rho(h_i)^*) =$$

$$\phi(v, \sum_{i=1}^n \bar{a} \cdot \rho(h_i)^*).$$

Thus $\Phi(v, A) = \Phi(V, A)$. This computation also shows the last equation. \square

For every $w \in V$ there are $r, s \in R$ and $\bar{a} \in \bar{A}$ with $w = vr + \Phi(v, \bar{a}) + vs\mu$. Thus we can identify V with $R \times \bar{A} \times R$ and set $(r, \bar{a}, s) := vr + \Phi(v, \bar{a}) + vs\mu$.

Lemma 7.2 *Let $r, s \in R$ and $a, b \in A$. Then:*

- (a) $(r, \bar{a}, s)\mu = (-s, \bar{a}, r)$.
- (b) $(r, \bar{a}, s)b = (r + f(\bar{a}, \bar{b}) + s\rho(h_b), \bar{a} + \bar{b} \cdot s^*, s)$.

Proof.

$$\begin{aligned} \text{(a)} \quad (r, \bar{a}, s)\mu &= (vr + \Phi(v, \bar{a}) + vs\mu)\mu = vs\mu^2 + \Phi(v, \bar{a}) + vr\mu = \\ &= -vs + \Phi(v, \bar{a}) + vr\mu = (-s, \bar{a}, r). \end{aligned}$$

$$\begin{aligned} \text{(b)} \quad (r, \bar{a}, s)b &= (vr + [v\mu, a] - vh_a + vs\mu)b = \\ &= vr - vh_a + [v\mu, a] + [v\mu, a, b] + vs\mu + \Phi(vs, \bar{b}) + vs\rho(h_b) = \\ &= vr + vf(\bar{a}, \bar{b}) + vs\rho(h_b) + \Phi(v, \bar{b} \cdot s^*) + \Phi(v, \bar{a}) + vs\mu = \\ &= (r + f(\bar{a}, \bar{b}) + s\rho(h_b), \bar{a} + \bar{b} \cdot s^*, s). \end{aligned}$$

\square

We will now define a R -vectorspace structure on V : For $\bar{a} \in \bar{A}$ set $(r, \bar{a}, s) \circ \lambda = (\lambda^*r, \bar{a} \cdot \lambda, \lambda^*s)$. Then we have

Proposition 7.3 *(a) \circ defines a scalar multiplication of R on V .*

(b) \circ commutes with the action of G on V .

Proof.

- (a) This can be easily verified.
- (b) We only have to show that $(w \circ \lambda)\mu = w\mu \circ \lambda$ and $(w \circ \lambda)b = wb \circ \lambda$ for all $b \in A$ and all $\lambda \in R$ hold. If $r, s \in R, \bar{a} \in \bar{A}$, then

$$\begin{aligned} ((r, \bar{a}, s) \circ \lambda)\mu &= (\lambda^*r, \bar{a} \cdot \lambda, \lambda^*s)\mu = (-\lambda^*s, \bar{a} \cdot \lambda, \lambda^*r) \\ &= (-s, \bar{a}, r) \circ \lambda = ((r, \bar{a}, s)\mu) \circ \lambda. \end{aligned}$$

Moreover,

$$\begin{aligned}
((r, \bar{a}, s) \circ \lambda)b &= (\lambda^* r, \bar{a} \cdot \lambda, \lambda^* s)b \\
&= (\lambda^* r + f(\bar{a} \cdot \lambda, \bar{b}) + \lambda^* s \rho(h_b), \bar{a} \cdot \lambda + \bar{b} \cdot (\lambda^* s)^*, \lambda^* s) = \\
&\quad (\lambda^* (r + f(\bar{a}, \bar{b}) + s \rho(h_b)), (\bar{a} + \bar{b} \cdot s^*) \cdot \lambda, \lambda^* s) \\
&= ((r + f(a, b) + s \rho(h_b), \bar{a} + \bar{b} \cdot s^*, s) \circ \lambda) = ((r, \bar{a}, s)b) \circ \lambda.
\end{aligned}$$

□

For $r, s \in R$ and $\bar{a} \in \bar{A}$ set $[r, \bar{a}, s] = (r^*, \bar{a}, s^*)$. Then we have

$$[r, \bar{a}, s] \circ \lambda = (\lambda^* r^*, \bar{a} \cdot \lambda, \lambda^* s^*) = [r\lambda, \bar{a} \cdot \lambda, s\lambda],$$

$$[r, \bar{a}, s]\mu = (r^*, \bar{a}, s^*)\mu = (-s^*, \bar{a}, r^*) = [-s, \bar{a}, r]$$

and

$$\begin{aligned}
[r, \bar{a}, s]b &= (r^*, \bar{a}, s^*)b = (r^* + f(\bar{a}, \bar{b}) + s^* \rho(h_b), \bar{a} + \bar{b} \cdot s, s^*) = \\
&\quad [r - f(\bar{b}, \bar{a}) + \rho(h_b)^* s, \bar{a} + \bar{b} \cdot s, s].
\end{aligned}$$

Theorem 7.4 *Let $\pi : V \rightarrow R/J : \pi([r, \bar{a}, s]) = s^* r + \rho(h_a) + J$. Then π is a pseudo-quadratic form of Witt index 1 and $G = SU(\pi)$.*

Proof. Since $\bar{a} \rightarrow \rho(h_a) + J$ is an anisotropic form of \bar{A} , we get that the map $\pi : V \rightarrow R/J$ is a pseudo-quadratic form of Witt index 1 (see 3.3). Using the notation of 3.3, one can see that $a = \alpha_{(\bar{a}, \rho(h_a))}$. If $b \in B$, then $b = a^\mu$ for an element $a \in A$, and thus $b = \alpha_{(\bar{a}, \rho(h_a))}^\mu = \beta_{(x, t)}$ with $x \in V$ and $t \in K$. Thus the claim follows. □

We sum up our results in our main theorem.

Theorem 7.5 *Let G be a rank one group with unipotent subgroups A and B . Suppose V is a cubic module for G with $[V, G] = V$ and $C_V(G) = 0$. If $A_0 \neq 1$ and the Jordan division algebra J defined by $\rho(H_0)$ is not commutative, then $J = H_0(K, *)$ for a skewfield K with involution $*$ such that $\langle J \rangle = K$, a K -vectorspace M and a pseudo-quadratic form $\pi : M \rightarrow K/J$ of Witt index 1 such that $G \cong SU(\pi)$. Moreover, there are G -submodules U, W of V with $U \leq W$ and $W/U \cong M$ as G -module. V is a direct sum of G -submodules isomorphic to M except $\text{char} K = 2$ and one of the following hold:*

- (a) K is a quaternion algebra.
- (b) K is a biquaternion algebra, $*$ a symplectic involution on K and $J = K_*$.

Corollary 7.6 *Suppose that k , G , M and Σ are as in 3.7. Then either $\langle A, B \rangle$ for $A, B \in \Sigma$ distinct is isomorphic to $SL_2(F)$ for an extension field F of k or there is a skewfield $K \subseteq \text{End}_G(M)$, an involution $*$ of K with $\langle K_* \rangle = K$, an irreducible submodule M_0 of M and a $*$ -skew-hermitian form $f : M_0 \times M_0 \rightarrow K$ of Witt index 1 such that $G \cong SU(M_0, f)$. Moreover, M is a direct sum of copies of M_0 .*

Proof. If A and B are two distinct elements in Σ and $U(A), U(B)$ are defined as in 3.7, then $G = \langle U(A), U(B) \rangle$ and G acts cubically on M with $U(A)_0 = A$ and $U(B)_0 = B$. By our main theorem, either $\langle A, B \rangle \cong SL_2(F)$ for an extension field F of k , or there is a skewfield K with involution $*$ such that K_* generates K , an irreducible submodule M_0 of M and a pseudo-quadratic form $\pi : M_0 \rightarrow K/K_*$ with $G = SU(\pi)$. Since $\text{char } k \neq 2$, π is uniquely determined by its corresponding skew-hermitian form f . Since $\text{char } k \neq 2$, M is the direct sum of copies of M_0 . \square

If G can be generated by three elements of Σ , then this already follows from Theorem 2 of [18]. Note that if $K = \mathbb{H}$ and $*$ is defined by $r^* = -ir^\sigma i$, where σ is the standard involution of \mathbb{H} and $i^2 = -1$, then any hermitian form proportional to a $*$ -skew-hermitian form is σ -hermitian. But $K_\sigma = Z(K)$ doesn't generate K . Thus we cannot replace "skew-hermitian" by "hermitian" in our corollary.

References

- [1] R. Baer, Radical ideals, Am. J. Math. 65, 537-568 (1943).
- [2] A. Borovik, A. Nésin, Groups of finite Morley rank, Oxford Logic Guides, Clarendon Press, Oxford (1994)
- [3] T. De Medts, Moufang sets arising from Moufang polygons of type E_6 and E_7 , unpublished, available on <http://java.ugent.be/~tdemedts/research.php>
- [4] T. De Medts and Y. Segev, Identities in Moufang sets, Trans. Amer. Math. Soc. 360, No. 11, 5831-5852 (2008)
- [5] T. De Medts, R. Weiss, Moufang sets and Jordan division algebras, Math. Ann. 335, No. 2, 415-433 (2006)
- [6] M. Grüninger, Special Moufang sets with Abelian Hua subgroup, J. Algebra 323, No. 6, 1797-1801 (2010)
- [7] I. N. Herstein, Rings with involution, Chicago Lectures in Mathematics, Chicago London, The University of Chicago Press (1976).
- [8] L. K. Hua, On the automorphisms of a field, Proc. Natl. Acad. Sci. USA 35 (1949), 386-389

- [9] R. Knop, The Geometry of Moufang sets, Dissertation, Martin-Luther-Universität Halle-Wittenberg (2005))
- [10] K. McCrimmon, The Zelmanov approach to Jordan homomorphisms of associative algebras, *Journal of Algebra* 123 (1989), 457-477
- [11] K. McCrimmon, E. Zel'manov, The structure of strongly prime Jordan division algebras, *Advances in Mathematics* 69, 133-222 (1988)
- [12] Y. Segev, Proper Moufang sets with abelian root groups are special, *J. Amer. Math. Soc.* 22 (2009), 889-908.
- [13] W. R. Scott, Group theory, Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1964
- [14] Y. Segev, R. Weiss, On the action of the Hua subgroups in special Moufang set, *Math. Proc. Camb. Philos. Soc.* 144, No. 1, 77-84 (2008).
- [15] F. G. Timmesfeld, Abstract root subgroups and quadratic action. With an Appendix by A. E. Zalesskii, *Adv. Math.* 142, No.1 (1999), 1-150
- [16] F. G. Timmesfeld, Abstract root subgroups and simple groups of Lie-type, Birkhäuser, Monographs in Mathematics. 95, Basel, 2001
- [17] F. G. Timmesfeld, Quadratic rank-one groups and quadratic Jordan algebras, *Proc. London Math. Soc.* (3) 95 (2007), 156-178
- [18] F. G. Timmesfeld, Quadratic pairs without commuting root subgroups, *Journal of Algebra* 318, 111-134 (2007)
- [19] J. Tits, R. M. Weiss, Moufang Polygons, Springer Monographs in Mathematics, Springer-Verlag, Berlin, Heidelberg, New York, 2002.